



DS-900WN DS-800WN

Administratorhåndbok

Nødvendige innstillinger som passer til ditt formål

Nettverksinnstillinger

Nødvendige innstillinger for skanning

Grunnleggende sikkerhetsinnstillinger

Avanserte sikkerhetsinnstillinger

Bruke Epson Open Platform

Opphavsrett

Ingen deler av denne publikasjonen kan reproduseres, lagres i et gjenfinningssystem eller overføres i noen form eller på noen måte, elektronisk, mekanisk, ved fotokopiering, innspilling eller annet, uten skriftlig forhåndstillatelse fra Seiko Epson Corporation. Ingen patentansvar forutsatt med hensyn til bruk av informasjonen i dette dokumentet. Det tas heller ikke noe ansvar for skader som følge av bruk av informasjonen i dette dokumentet. Informasjonen i dette dokumentet er kun beregnet for bruk av dette Epson-produktet. Epson er ikke ansvarlig for bruk av denne informasjonen i forbindelse med andre produkter.

Verken Seiko Epson Corporation eller dets datterselskaper er ansvarlig overfor kjøperen av dette produktet eller tredjeparter for skader, tap, kostnader eller utgifter som kjøper eller tredjepart som følge av ulykke, feil bruk eller misbruk av dette produktet eller uautoriserte modifikasjoner, reparasjoner eller endringer på dette produktet, eller (unntatt i USA) manglende overholdelse av Seiko Epson Corporations drifts- og vedlikeholdsinstruksjoner.

Seiko Epson Corporation og dets datterselskaper kan ikke holdes ansvarlig for skader eller problemer som oppstår ved bruk av tilleggsutstyr eller noen forbruksprodukter andre enn dem som er angitt som originale Epson-produkter eller Epson-godkjente produkter av Seiko Epson Corporation.

Seiko Epson Corporation skal ikke holdes ansvarlig for eventuelle skader som følge av elektromagnetiske forstyrrelser som oppstår ved bruk av andre grensesnittkabler enn de som er angitt som Epson-godkjente produkter av Seiko Epson Corporation.

© 2024 Seiko Epson Corporation

Innholdet i denne håndboken og spesifikasjonene for dette produktet kan endres uten varsel.

Varemerker

- Microsoft, Windows, Windows Server, Microsoft Edge, SharePoint, and Internet Explorer are trademarks of the Microsoft group of companies.
- Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- Chrome, Chromebook and Android are trademarks of Google LLC.
- Wi-Fi®, Wi-Fi Direct®, and Wi-Fi Protected Access® are registered trademarks of Wi-Fi Alliance®. Wi-Fi Protected Setup™, WPA2™, WPA3™ are trademarks of Wi-Fi Alliance®.
- The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- The Mopria™ word mark and the Mopria™ Logo are registered and/or unregistered trademarks of Mopria Alliance, Inc. in the United States and other countries. Unauthorized use is strictly prohibited.
- Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- Generell melding: alle andre varemerker tilhører de respektive eierne og brukes kun i sammenheng med identifisering.

Innholdsfortegnelse

Opphavsrett

Varemerker

Innledning

Innholdet i dette dokumentet.	7
Bruk av denne guiden.	7
Merker og symboler.	7
Beskrivelser brukt i denne bruksanvisningen.	7
Operativsystemreferanser.	7

Merknader om administratorpassordet

Merknader om administratorpassordet.	10
Opprinnelig administratorpassord.	10
Operasjoner som krever administratorpassordet.	10
Endre administratorpassordet.	10
Tilbakestille administratorpassordet.	10

Nødvendige innstillinger som passer til ditt formål

Nødvendige innstillinger som passer til ditt formål.	12
--	----

Nettverksinnstillinger

Koble skanneren til nettverket.	15
Før tilkobling til nettverket.	15
Koble til nettverket fra kontrollpanelet.	17
Legge til eller skifte ut datamaskinen eller enheter.	21
Koble til en skanner som er koblet til nettverket.	21
Koble til en smartenhet og skanner direkte (Wi-Fi Direct).	23
Tilbakestille nettverkstilkoblingen.	25
Kontrollere statusen for nettverkstilkoblingen.	27
Kontrollere status for nettverkstilkoblingen fra kontrollpanelet.	27
Nettverksspesifikasjoner.	28
Wi-Fi-spesifikasjoner.	28
Ethernet-spesifikasjoner.	30
Nettverksfunksjoner og støtte for IPv4/IPv6.	30
Sikkerhetsprotokoll.	31
Bruke porten for skanneren.	31
Problemløsning.	32

Kan ikke koble til et nettverk.	32
---	----

Programvare for å konfigurere skanneren

Program for konfigurering av skanneoperasjoner (Web Config).	37
Slik kjører du Web Config i en nettleser.	37
Epson Device Admin.	38
Konfigurasjonsmal.	39

Nødvendige innstillinger for skanning

Registrere en e-postserver.	44
Kontrollere tilkoblingen til en e-postserver.	45
Opprette en nettverksmappe.	46
Gjøre kontakter tilgjengelig.	53
Sammenlikning av kontaktkonfigurering.	54
Registrere et mål for kontakter ved hjelp av Web Config.	54
Registrere mål som en gruppe med Web Config.	56
Sikkerhetskopiere og importere kontakter.	57
Eksportering og grupperegistrering av kontakter med verktøyet.	58
Samarbeid mellom LDAP-server og brukere.	59
Konfigurere AirPrint.	62
Problemer ved forberedelse av nettverksskanning.	63
Hint for å løse problemer.	63
Får ikke tilgang til Web Config.	63

Tilpasse kontrollpanelskjermen

Registrere Forhåndsinn.	67
Menyalternativer for Forhåndsinn.	68
Redigere startskjermen til kontrollpanelet.	69
Endre Layout på startskjermen.	69
Legg til ikon.	70
Fjern ikon.	71
Flytt ikon.	72

Grunnleggende sikkerhetsinnstillinger

Introduksjon til produktets sikkerhetsfunksjoner.	74
Administratorinnstillinger.	74
Konfigurere administratorpassordet.	74

Bruke Låsinnstilling for kontrollpanelet.	76
Logge på som en administrator fra kontrollpanelet.	79
Begrense tilgjengelige funksjoner (Tilgangskontroll).	80
Opprette brukerkontoen.	80
Aktivere Tilgangskontroll.	81
Logge på en skanner der Tilgangskontroll er aktivert.	81
Deaktivere eksternt grensesnitt.	82
Aktivere programverifisering ved oppstart.	82
Deaktivere nettverksskanning fra datamaskinen.	83
Aktivere eller deaktivere WSD-skanning.	83
Administrere en ekstern skanner.	84
Sjekke informasjon for en ekstern skanner.	84
Motta e-postvarslinger når det skjer hendelser.	84
Bruke Web Config til å kontrollere skannerens strømforsyning.	85
Gjenopprette standardinnstillingene.	85
Informasjon om Epson Remote Services.	86
Problemløsning.	86
Glemt administratorpassordet ditt.	86

Avanserte sikkerhetsinnstillinger

Sikkerhetsinnstillinger og forebygging av farlige situasjoner.	88
Innstilling av sikkerhetsfunksjoner.	89
Kontrollere med protokoller.	89
Kontrollprotokoller.	89
Protokoller du kan Aktivere eller Deaktivere.	89
Innstillingselementer for protokoll.	90
Bruke et digitalt sertifikat.	92
Om digital sertifisering.	92
Konfigurere et CA-signert sertifikat.	92
Oppdatere et selvsignert sertifikat.	96
Konfigurere et CA-sertifikat.	96
SSL/TLS-kommunikasjon med skanneren.	97
Konfigurere grunnleggende SSL/TLS-innstillinger.	97
Konfigurere et serversertifikat for skanneren.	98
Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering.	98
Om IPsec/IP-filtrering.	98
Konfigurere standardpolicy.	99
Konfigurere gruppepolicy.	102
Eksempler på IPsec/IP-filtrering.	108
Konfigurere et sertifikat for IPsec/IP-filtrering.	109
Koble skanneren til et IEEE802.1X-nettverk.	109

Konfigurere et IEEE 802.1X-nettverk.	109
Konfigurere et sertifikat for IEEE 802.1X.	111
Løse problemer med avanserte sikkerhetsinnstillinger.	111
Gjenopprette sikkerhetsinnstillingene.	111
Problemer ved bruk av funksjoner for nettverkssikkerhet.	112
Problemer med å bruke et digitalt sertifikat.	114

Bruke Epson Open Platform

Oversikt over Epson Open Platform.	119
Konfigurere Epson Open Platform.	119
Bekreftede Epson Open Platform.	119

Montere en godkjenningseenhet

Koble til en godkjenningseenhet.	121
Driftssjekk for godkjenningseenheter.	121
Bekreftede at godkjenningsskortet gjenkjennes.	121
Feilsøke godkjenningseenheten.	122
Kan ikke lese godkjenningsskortet.	122

Vedlikehold

Rengjøre utsiden av skanneren.	124
Rengjøre innsiden av skanneren.	124
Bytte ut rullersettet.	129
Koder for rullersett.	134
Tilbakestill antall skanninger etter å ha byttet ut rullen.	134
Energisparing.	135
Transportere skanneren.	135
Sikkerhetskopier innstillingene.	136
Eksportere innstillingene.	136
Importere innstillingene.	137
Gjenopprett standardinnst.. . . .	137
Oppdatere programmer og fastvare.	138
Oppdatere skannerens fastvare ved hjelp av kontrollpanelet.	139
Oppdatere fastvaren ved å bruke Web Config.	139
Oppdatere fastvaren uten å koble til Internett.	139

Innledning

Innholdet i dette dokumentet.	7
Bruk av denne guiden.	7

Innholdet i dette dokumentet

Dette dokumentet oppgir følgende informasjon for skanneradministratorer.

- Nettverksinnstillinger
- Forberede skannefunksjonen
- Aktivere og administrere sikkerhetsinnstillinger
- Utføre daglig vedlikehold

For standardmetodene for å bruke skanneren, kan du se *Brukerhåndbok*.

Bruk av denne guiden

Merker og symboler



Forsiktig:

Instruksjoner som må følges nøye for å unngå personskade.



Forsiktighetsregel:

Instruksjoner som må overholdes for å unngå skade på utstyret.

Merknad:

Gir supplerende og referanseinformasjon.

Relatert informasjon

➔ Lenker til relaterte avsnitt.

Beskrivelser brukt i denne bruksanvisningen

- Skjermbilder for programmene er fra Windows 10 eller macOS High Sierra. Innholdet vist på skjermene varierer avhengig av modell og situasjon.
- Illustrasjonene som er brukt i denne bruksanvisningen er kun for referanse. Selv om de kan avvike noe fra det faktiske produktet, er driftsmetodene de samme.

Operativsystemreferanser

Windows

I denne brukerhåndboken refererer "Windows 11", "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Server 2022", "Windows Server 2019", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012", "Windows Server 2008 R2" og "Windows Server 2008" til følgende operativsystemer. I tillegg brukes «Windows» for å referere til alle versjoner.

- Microsoft® Windows® 11 operativsystem
- Microsoft® Windows® 10 operativsystem
- Microsoft® Windows® 8.1 operativsystem
- Microsoft® Windows® 8 operativsystem
- Microsoft® Windows® 7 operativsystem
- Microsoft® Windows Server® 2022 operativsystem
- Microsoft® Windows Server® 2019 operativsystem
- Microsoft® Windows Server® 2016 operativsystem
- Microsoft® Windows Server® 2012 R2 operativsystem
- Microsoft® Windows Server® 2012 operativsystem
- Microsoft® Windows Server® 2008 R2 operativsystem
- Microsoft® Windows Server® 2008 operativsystem

Mac OS

I denne håndboken brukes «Mac OS» for å hen vise til Mac OS X 10.9 eller nyere samt macOS 11 eller nyere.

Merknader om administratorpassordet

Merknader om administratorpassordet.	10
Opprinnelig administratorpassord.	10
Operasjoner som krever administratorpassordet.	10
Endre administratorpassordet.	10
Tilbakestille administratorpassordet.	10

Merknader om administratorpassordet

På denne enheten kan du angi et administratorpassord for å hindre at uautoriserte tredjeparter som er koblet til et nettverk får tilgang til eller endrer enhets- eller nettverksinnstillingene som er lagret på enheten.

Hvis du angir et administratorpassord, må dette passordet angis for å endrer innstillinger i konfigurasjonsprogramer, for eksempel i Web Config.

Det opprinnelige administratorpassordet er angitt på skanneren, men du kan endre det til et hvilket som helst passord.

Opprinnelig administratorpassord

Det opprinnelige administratorpassordet varierer avhengig av etiketten på produktet. Hvis det er en PASSWORD-etikett på baksiden, angir du det 8-sifrede nummeret på etiketten. Hvis det ikke er en PASSWORD-etikett der, angir du serienummeret på etiketten på baksiden av produktet som administratorpassord den første gangen.

Vi anbefaler å endre det opprinnelige administratorpassordet fra standardpassordet.

Merknad:

Ingen brukernavn er angitt som standard.

Operasjoner som krever administratorpassordet

Hvis du blir bedt om å angi administratorpassordet i løpet av følgende operasjoner, skriver du inn administratorpassordet som er angitt på produktet.

- Når du logger på de avanserte innstillingene for Web Config
- Når du bruker en meny på kontrollpanelet som er låst av administratoren
- Når du endrer enhetsinnstillingene i programmet
- Når du oppdaterer fastvaren for enheten
- Når du endrer eller tilbakestiller administratorpassordet

Endre administratorpassordet

Du kan endre fra produktets kontrollpanel eller i Web Config.

Når du endrer passordet, må det nye passordet være mellom 8 og 20 tegn langt og inneholde kun alfanumeriske tegn og symboler med én byte.

Tilbakestille administratorpassordet

Du kan tilbakestille administratorpassordet til den opprinnelige innstillingen fra produktets kontrollpanel eller i Web Config.

Hvis du har glemt passordet og ikke kan tilbakestille det til standardinnstillingene, må produktet inn til reparasjon. Kontakt lokalforhandleren.

Nødvendige innstillinger som passer til ditt formål

Nødvendige innstillinger som passer til ditt formål. 12

Nødvendige innstillinger som passer til ditt formål

Se det følgende for å gjøre nødvendige endringer for å passe formålet ditt.

Koble skanneren til nettverket

Formål	Nødvendige innstillinger
Jeg vil koble skanneren til nettverket.	Sett opp skanneren din for nettverksskanning. "Koble skanneren til nettverket" på side 15
Jeg vil koble skanneren til en ny datamaskin.	Konfigurer nettverksinnstillingene for skanneren på den nye datamaskinen. "Legge til eller skifte ut datamaskinen eller enheter" på side 21

Innstillinger for skanning

Formål	Nødvendige innstillinger
Jeg vil sende skannede bilder via e-post. (Skann til e-post)	1. Konfigurer e-postserveren du vil koble til. "Registrere en e-postserver" på side 44 2. Registrer mottakerens e-postadresse i Kontakter (valgfritt). Ved å registrere e-postadressen trenger du ikke å skrive den inn hver gang du vil sende noe, du kan bare velge den fra kontaktene dine. "Gjøre kontakter tilgjengelig" på side 53
Jeg vil lagre skannede bilder til en mappe på et nettverk. (Skann til nettverksmappe /FTP)	1. Lag en mappe i nettverket der du vil lagre bildene. "Opprette en nettverksmappe" på side 46 2. Registrer banen til mappen i Kontakter (valgfritt). Ved å registrere mappebanen trenger du ikke å skrive den inn hver gang du vil sende noe, du kan bare velge den fra kontaktene dine. "Gjøre kontakter tilgjengelig" på side 53
Jeg vil lagre skannede bilder i en skytjeneste. (Skann til nettsky)	Konfigurer Epson Connect. Se nettsiden til Epson Connect-portalen for mer informasjon om oppsettet. Du trenger en brukerkonto for den nettbaserte lagringstjenesten du vil koble til når du stiller dette inn. https://www.epsonconnect.com/ http://www.epsonconnect.eu (kun Europa)

Tilpasse kontrollpanelskjermen

Formål	Nødvendige innstillinger
Jeg vil endre det som vises på skannerens kontrollpanel.	Angi Forhåndsinn eller Rediger Startskjerm . Du kan registrere favorittskanneinnstillinger på kontrollpanelet og redigere elementene som vises. "Tilpasse kontrollpanelskjermen" på side 66

Angi grunnleggende sikkerhetsfunksjoner

Formål	Nødvendige innstillinger
Jeg vil unngå at andre enn administratoren kan endre skanneinnstillingene.	Angi et administratorpassord for skanneren. "Administratorinnstillinger" på side 74
Jeg vil deaktivere bruk av skannere med USB-tilkobling.	Deaktiver det eksterne grensesnittet. "Deaktiver eksternt grensesnitt" på side 82

Angi avanserte sikkerhetsfunksjoner

Formål	Nødvendige innstillinger
Jeg vil kontrollere hvilke protokoller som brukes.	Aktiverer eller deaktiver protokollene. "Kontrollere med protokoller" på side 89
Jeg vil kryptere kommunikasjonsbanen.	1. Konfigurer et digitalt sertifikat. "Bruke et digitalt sertifikat" på side 92 2. Konfigurer SSL/TLS-kommunikasjon. "SSL/TLS-kommunikasjon med skanneren" på side 97
Jeg vil bruke kryptert kommunikasjon (IPsec). Jeg vil kunne bruke programvaren kun fra én bestemt datamaskin (IP-filtrering).	Konfigurere policyer for å filtrere trafikk. "Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering" på side 98
Jeg vil bruke en skanner i et IEEE802.1X-nettverk.	Konfigurer IEEE802.1X for skanneren. "Koble skanneren til et IEEE802.1X-nettverk" på side 109

Synkronisere skanneren med et autentiseringssystem

Få en produktnøkkel fra det dedikerte nettstedet og aktiver Epson Open Platform på skanneren din.

["Bruke Epson Open Platform" på side 118](#)

Bruke et godkjenningalternativ (Epson Print Admin/Epson Print Admin Serverless)

Du trenger en lisensnøkkel for tast å bruke dette alternativet.

Kontakt forhandleren for mer informasjon.

Merknad:

Du kan ikke bruke Epson Print Admin Serverless når systemet er synkronisert med Epson Open Platform.

Nettverksinnstillinger

Koble skanneren til nettverket.	15
Legge til eller skifte ut datamaskinen eller enheter.	21
Kontrollere statusen for nettverkstilkoblingen.	27
Nettverksspesifikasjoner.	28
Problemløsning.	32

Koble skanneren til nettverket

Denne delen forklarer hvordan du kobler skanneren til nettverket ved hjelp av skannerens kontrollpanel.

Merknad:

Hvis skanneren og datamaskinen er i samme segment, kan du også koble til ved hjelp av installasjonsprogrammet.

Åpne den følgende nettsiden og tast inn produktnavnet for å starte installasjonsprogrammet. Gå til **Oppsett**, og start konfigureringen.

<https://epson.sn>

Du kan se bruksanvisningene i Web-filmhåndbøker. Åpne følgende URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Før tilkobling til nettverket

For å koble til nettverket må du kontrollere tilkoblingsmetoden og informasjonen om innstilling for tilkoblingen på forhånd.

Informasjonssamling i tilkoblingsinnstilling

Klargjør nødvendig konfigureringinformasjon for å koble til. Kontroller følgende informasjon på forhånd.

Divisjoner	Artikler	Merk
Enhetens tilkoblingsmetode	<input type="checkbox"/> Ethernet <input type="checkbox"/> Wi-Fi	Fastslå hvordan skanneren skal kobles til nettverket. Koble til LAN-bryteren for kablet LAN. Koble til tilgangspunktets nettverk (SSID) for Wi-Fi.
LAN-tilkoblingsinformasjon	<input type="checkbox"/> IP-adresse <input type="checkbox"/> Nettverksmaske <input type="checkbox"/> Standard gateway	Fastslå IP-adressen som skal tilordnes til skanneren. Når du tilordner IP-adressen statisk, er alle verdier nødvendige. Når du tilordner IP-adressen automatisk ved hjelp av DHCP-funksjonen, er ikke denne informasjonen nødvendig fordi den angis automatisk.
Wi-Fi-tilkoblingsinformasjon	<input type="checkbox"/> SSID <input type="checkbox"/> Passord	Dette er SSID-en (nettverksnavnet) og passordet til tilgangspunktet som skanneren kobler seg til. Hvis filtrering av MAC-adresse har blitt angitt, må skannerens MAC-adresse registreres på forhånd for å registrere skanneren. Se følgende for støttede standarder. "Nettverksspesifikasjoner" på side 28
DNS-serverinformasjon	<input type="checkbox"/> IP-adresse for primær DNS <input type="checkbox"/> IP-adresse for sekundær DNS	Disse kreves når du spesifiserer DNS-servere. Den sekundære DNS-en angis når systemet har overflødig konfigurering og det finnes en sekundær DNS-server. Hvis du er i en liten organisasjon og ikke angir DNS-serveren, angis routerens IP-adresse.

Divisjoner	Artikler	Merk
Proxy-serverinformasjon	<input type="checkbox"/> Proxy-servernavn	Angi dette når nettverksmiljøet bruker proxyserveren til å få tilgang til Internett fra intranettet og du bruker funksjonen som kobler skanneren direkte til Internett. For følgende funksjoner kobles skanneren direkte til Internett. <input type="checkbox"/> Epson Connect-tjenester <input type="checkbox"/> Skytjenester fra andre selskaper <input type="checkbox"/> Fastvareoppdatering <input type="checkbox"/> Sende skannede bilde til SharePoint(WebDAV)
Portnummerinformasjon	<input type="checkbox"/> Frigjøring av portnummer	Kontroller portnummeret som brukes av skanneren og datamaskinen, og frigjør porten som er blokkert av en brannmur hvis nødvendig. Se følgende for portnummeret som brukes av skanneren. "Bruke porten for skanneren" på side 31

Tildeling av IP-adresse

Dette er de følgende typer IP-adressetildeling.

Statisk IP-adresse:

Tildel forhåndsbestemt IP-adresse til skanneren (vert) manuelt.

Informasjonen om å koble til nettverket (delnettmaske, standard gateway, DNS-server og så videre) må angis automatisk.

IP-adressen endres ikke når enheten slås av, noe som er nyttig når du ønsker å administrere enheter med et miljø hvor du ikke kan endre IP-adresse, eller du ønsker å administrere enheter ved hjelp av IP-adressen. Vi anbefaler innstillinger for skanneren, serveren, osv., som mange datamaskiner bruker. Når sikkerhetsfunksjoner som IPsec/IP-filtrering brukes, må du tildele en fast IP-adresse slik at IP-adressen ikke endres.

Automatisk tildeling ved hjelp av DHCP-funksjonen (dynamisk IP-adresse):

Tildel IP-adressen automatisk til skanneren (vert) ved hjelp av DHCP-funksjonen til DHCP-serveren eller -routeren.

Informasjonen om å koble til nettverket (delnettmaske, standard gateway, DNS-server og så videre) angis automatisk, så du kan enkelt koble enheten til nettverket.

Hvis enheten eller routeren er slått av, eller avhengig av DHCP-serverens innstillinger, kan IP-adressen endres ved ny tilkobling.

Vi anbefaler å administrere enheter med annet enn IP-adressen og kommunisere med protokoller som kan følge IP-adressen.

Merknad:

Når du bruker DHCP-ens reservasjonsfunksjon for IP-adresse, kan du når som helst tildele samme IP-adresse til enhetene.

DNS-server og proxy-server

DNS-serveren har et vertsnavn, domenenavn for e-postadressen osv., i forbindelse med IP-adresseinformasjonen.

Kommunikasjon er ikke mulig hvis den andre parten beskrives av vertsnavnet, domenenavnet osv., når datamaskinen eller skanneren utfører IP-kommunikasjon.

Spør DNS-serveren om den informasjonen og får IP-adressen til den andre parten. Denne prosessen kalles navneløsning.

Derfor kan enheter som datamaskiner og skannere kommunisere ved hjelp av IP-adressen.

Navneløsning er nødvendig for at skanneren skal kunne kommunisere ved hjelp av e-postfunksjonen eller funksjonen for Internet-tilkobling.

Når du bruker disse funksjonene, må innstillingene for DNS-server angis.

Når du tilordner skannerens IP-adresse ved hjelp av DHCP-funksjonen til DHCP-serveren eller -routeren, angis dette automatisk.

Proxy-serveren er plassert på gateway mellom nettverket og Internett, og kommuniserer til datamaskinen, skanner og Internett (motsatt server) på vegne av hver av dem. Den motsatte serveren kommuniserer bare til proxy-serveren. Derfor vil skannerinformasjon som IP-adresse og portnummer kanskje ikke leses, noe som er forbundet med økt sikkerhet.

Når du kobler til Internett via proxyserver, må proxyserveren konfigureres på skanneren.

Koble til nettverket fra kontrollpanelet

Koble skanneren til nettverket ved å bruke kontrollpanelet på skanneren.

Tilordne IP-adressen

Still inn de grunnleggende elementene, for eksempel vertsadresse, Nettverksmaske eller Standard gateway.

Denne seksjonen forklarer prosedyren for hvordan du angir en statisk IP-adresse.

1. Slå på skanneren.
2. Velg **Innst.** på startskjermen til skannerens kontrollpanel.
3. Velg **Nettverksinnstillinger > Avansert > TCP/IP.**
4. Velg **Manuell** ved **Skaff IP-adresse.**

Når du stiller inn IP-adresse automatisk ved å bruke DHCP-funksjonen på ruter, velger du **Auto**. I slikt tilfelle stilles også **IP-adresse**, **Nettverksmaske** og **Standard gateway** i trinn 5 til 6 inn automatisk. Gå derfor til trinn 7.

5. Skriv inn IP-adressen.

Fokus flyttes til fremste eller bakerste segment separert med punktum hvis du velger ◀ og ▶.

Bekreft verdien som ble vist på forrige skjerm.

6. Konfigurer **Nettverksmaske** og **Standard gateway.**

Bekreft verdien som ble vist på forrige skjerm.



Forsiktighetsregel:

Hvis kombinasjonen av IP-adresse, Nettverksmaske og Standard gateway er feil, blir **Start oppsett** inaktiv og vil ikke kunne fortsette med innstillingene. Kontroller at alt som er skrevet inn er riktig.

7. Skriv inn IP-adressen for den primære DNS-serveren.

Bekreft verdien som ble vist på forrige skjerm.

Merknad:

Når du velger **Auto** i innstillingene for tilordning av IP-adresse, kan du velge DNS-serverinnstillinger fra **Manuell** eller **Auto**. Hvis du ikke kan hente DNS-server automatisk, velger du **Manuell** og angir DNS-serveradresse. Deretter skriver du sekundær DNS-serveradresse direkte inn. Hvis du velger **Auto**, går du til trinn 9.

8. Skriv inn IP-adressen for den sekundære DNS-serveren.

Bekreft verdien som ble vist på forrige skjerm.

9. Trykk **Start oppsett**.

Angi proxy-server

Konfigurer proxyserveren hvis begge av følgende er sant.

- Proxyserveren er bygget for Internett-tilkobling.
- Ved bruk av en funksjon hvor en skanner kobler direkte til Internett, som Epson Connect-tjenester eller andre selskapers skytjenester.

1. Velg **Innst.** på startskjermen.

Når du angir innstillinger etter innstilling av IP-adresse, vises **Avansert**-skjermen. Gå til trinn 3.

2. Velg **Nettverksinnstillinger > Avansert**.

3. Velg **Proxyserver**.

4. Velg **Bruk ved Proxyserver-innst.**

5. Skriv inn adressen for proxy-serveren med IPv4- eller FQDN-format.

Bekreft verdien som ble vist på forrige skjerm.

6. Skriv inn portnummeret for proxy-serveren.

Bekreft verdien som ble vist på forrige skjerm.

7. Trykk **Start oppsett**.

Koble til Ethernet

Koble skanneren til nettverket ved å bruke en LAN-kabel, og kontroller tilkoblingen.

1. Koble sammen skanneren og huben (LAN-bryter) med en LAN-kabel.

2. Velg  på Hjem-skjermen.

3. Velg **Ruter**.

4. Sørg for at innstillingene for Tilkobling og IP-adresse stemmer.

5. Trykk **Lukk**.

Koble til trådløst LAN (Wi-Fi)

Du kan koble skanneren til trådløst LAN (Wi-Fi) på flere måter. Velg en tilkoblingsmetode som passer med miljøet og forholdene du bruker enheten i.

Hvis du kjenner informasjonen til den trådløse ruter, som SSID og passord, kan du angi innstillingene manuelt.

Hvis den trådløse ruter støtter WPS, kan du angi innstillinger ved hjelp av konfigurering med trykknapp.

Etter du har koblet skanneren til nettverket, kobler til skanneren fra enheten du vil bruke (datamaskin, smartenhet, nettbrett og så videre.)

Merknad ved bruk av en 5 GHz Wi-Fi-tilkobling

Dette produktet bruker vanligvis W52 (36-kanals) som kanal når du kobler til Wi-Fi Direct (Enkel AP). Siden kanalen for tilkobling til trådløst LAN (Wi-Fi) velges automatisk, kan kanalen som brukes variere når den brukes samtidig som en Wi-Fi Direct-tilkobling. Hvis kanalene er forskjellige, kan dataens kommunikasjon med skanneren gå saktere. Hvis den ikke forstyrrer med bruken, kobler du SSID til i frekvensbåndet for 2,4 GHz. I frekvensbåndet for 2,4 GHz samsvarer kanalene som brukes.

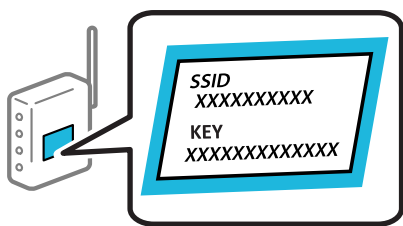
Når det trådløse nettverket settes til 5 GHz, anbefaler vi å deaktivere Wi-Fi Direct.


Angi Wi-Fi-innstillinger ved å angi SSID og passord

Du kan konfigurere et Wi-Fi-nettverk ved å angi nødvendig informasjon for å koble til en trådløs ruter fra skannerens kontrollpanel. Hvis du vil konfigurere ved hjelp av denne metoden, trenger du SSID og passord til en trådløs ruter.

Merknad:

Hvis du bruker en trådløs ruter med standard innstillinger, er SSID og passord angitt på etiketten. Hvis du ikke kjenner SSID-en og passordet, tar du kontakt med personen som konfigurerte den trådløse ruter, eller så kan du se i dokumentasjonen som fulgte med den trådløse ruter.



1. Trykk på  på startsidene.
2. Velg **Ruter**.
3. Trykk på **Start oppsett**.

Tilkoblingsdetaljene vises hvis nettverkstilkoblingen allerede er konfigurert. Trykk på **Bytt til Wi-Fi-tilkobling**, eller **Endre innstillinger** for å endre innstillingene.

4. Velg **Konfigurasjonveiledning for Wi-Fi**.

5. Følg instruksjonene på skjermen for å velge SSID-en, skrive inn passordet for den trådløse ruterer og starte oppsettet.

Hvis du vil sjekke skannerens tilkoblingsstatus til nettverket etter oppsett er fullført, kan du se lenken til relatert informasjon nedenfor hvis du vil ha mer informasjon.

Merknad:

- Hvis du ikke vet SSID-en, kan du se om det står skrevet på etiketten til trådløs-ruterer. Hvis du bruker trådløs-ruterens standardinnstillinger, bruker du SSID-en angitt på etiketten. Hvis du ikke finner noen informasjon, kan du se dokumentasjonen som fulgte med den trådløse ruterer.
- Det er forskjell på store og små bokstaver i passordet.
- Hvis du ikke vet passordet, kan du se om informasjonen står skrevet på etiketten til den trådløse ruterer. På etiketten er passordet gjerne oppgitt som «Network Key», «Wireless Password» eller lignende. Hvis du bruker standardinnstillingene til den trådløse ruterer, bruker du passordet som er skrevet på etiketten.
- Hvis du ikke kan se SSID-en du vil koble til, kan du bruke en programvare eller en app til å konfigurere Wi-Fi fra datamaskinen eller smartenheten din, som en smarttelefon eller et nettbrett. For å finne ut mer, skriv inn «<https://epson.sn>» i nettleseren din for å koble til nettsiden, skriv inn produktet og gå til **Oppsett**.

Relatert informasjon

➔ «Kontrollere statusen for nettverkstilkoblingen» på side 27

Utføre Wi-Fi-innstillinger med konfigurasjon med trykknapp (WPS)

Du kan konfigurere Wi-Fi-nettverk automatisk ved å trykke på en knapp på den trådløse ruterer. Du kan konfigurere med denne metoden hvis følgende betingelser er oppfylt.

- Den trådløse ruterer er kompatibel med WPS (Wi-Fi Protected Setup).
- Den gjeldende Wi-Fi-tilkoblingen har blitt etablert ved å trykke på en knapp på den trådløse ruterer.

Merknad:

Hvis du ikke finner knappen eller du konfigurere med programvaren, må du se dokumentasjonen som følger med den trådløse ruterer.

1. Trykk  på startskjermen.

2. Velg **Ruter**.

3. Trykk **Start oppsett**.

Tilkoblingsdetaljene vises hvis nettverkstilkoblingen allerede er satt opp. Trykk **Bytt til Wi-Fi-tilkobling**, eller **Endre innstillinger** for å endre innstillingene.

4. Velg **Trykknapp-oppsett (WPS)**.

5. Følg instruksjonene på skjermen.

Hvis du vil sjekke skannerens tilkoblingsstatus til nettverket etter oppsett er fullført, kan du se lenken til relatert informasjon nedenfor hvis du vil ha mer informasjon.

Merknad:


Hvis tilkoblingen mislykkes, starter du den trådløse ruterer på nytt, flytter den nærmere skanneren og prøver igjen.

Relatert informasjon

➔ «Kontrollere statusen for nettverkstilkoblingen» på side 27

Utføre Wi-Fi-innstillinger med konfigurasjon med PIN-kode (WPS)

Du kan automatisk koble til en trådløs ruter ved hjelp av en PIN-kode. Du kan bruke denne metoden til å konfigurere en trådløs ruter hvis den er kompatibel med WPS (Wi-Fi-beskyttet konfigurering). Bruk en datamaskin til å angi PIN-kode til den trådløse ruter.

1. Trykk  på startskjermen.
2. Velg **Ruter**.
3. Trykk **Start oppsett**.
Tilkoblingsdetaljene vises hvis nettverkstilkoblingen allerede er satt opp. Trykk **Bytt til Wi-Fi-tilkobling**, eller **Endre innstillinger** for å endre innstillingene.
4. Velg **Annet > Oppsett av PIN (WPS)**
5. Følg instruksjonene på skjermen.
Hvis du vil sjekke skannerens tilkoblingsstatus til nettverket etter oppsett er fullført, kan du se lenken til relatert informasjon nedenfor hvis du vil ha mer informasjon.

Merknad:

Se dokumentasjonen som følger med den trådløse ruter for å få mer informasjon om hvordan du angir PIN-kode.

Relatert informasjon

➔ [“Kontrollere statusen for nettverkstilkoblingen” på side 27](#)

Legge til eller skifte ut datamaskinen eller enheter

Koble til en skanner som er koblet til nettverket

Når skanneren allerede er koblet til nettverket, kan du koble en datamaskin eller en smartenhet til skanneren over nettverket.

Bruke en nettverksskanner fra en annen datamaskin

Vi anbefaler å bruke installasjonsprogrammet for å koble skanneren til en datamaskin.

Åpne den følgende nettsiden og tast inn produktnavnet for å starte installasjonsprogrammet. Gå til **Oppsett**, og start konfigurasjonen.

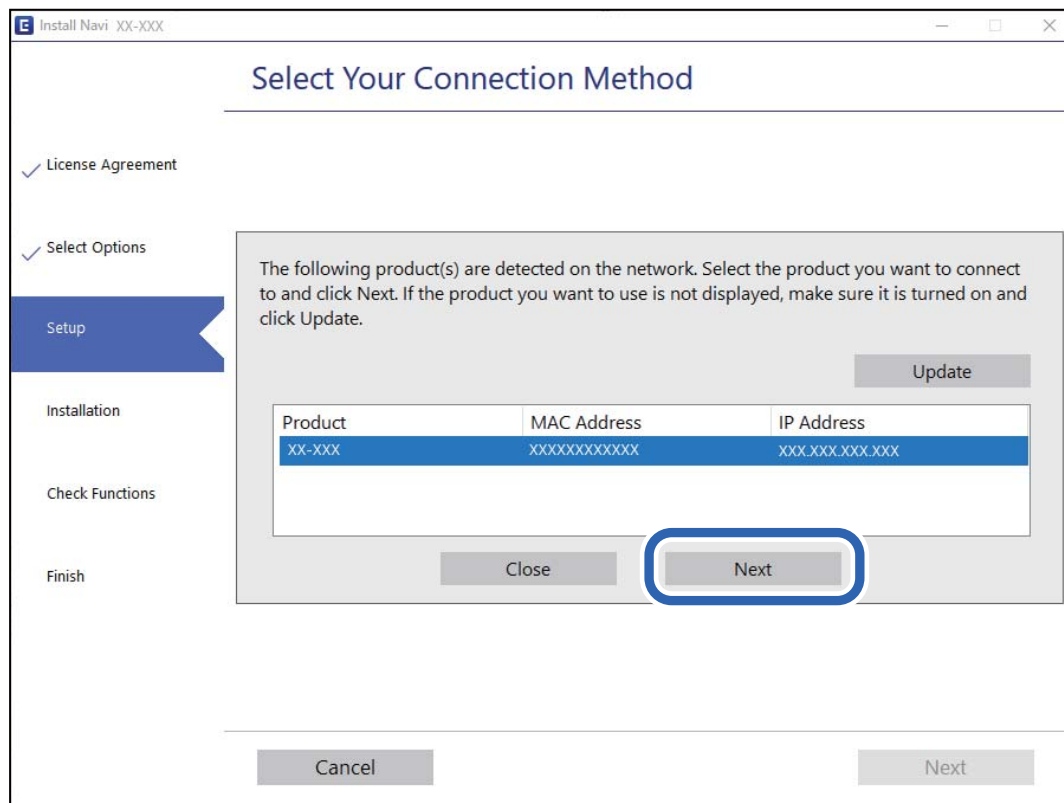
<https://epson.sn>

Du kan se bruksanvisningene i Web-filmhåndbøker. Åpne følgende URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Velge skanneren

Følg instruksjonene på skjermen helt til følgende skjerm vises, velg skannernavnet du vil koble til, og klikk deretter på **Neste**.



Følg instruksjonene på skjermen.

Bruke en nettverksskanner fra en smartenhet

Du kan koble en smartenhet til skanneren ved å bruke en av metodene nedenfor.

Koble til over en trådløs ruter

Koble smartenheten til samme Wi-Fi-nettverk (SSID) som skanneren.

Se følgende for mer informasjon.

[“Angi innstillinger for tilkobling til smartenheten” på side 26](#)

Koble til via Wi-Fi Direct

Koble smartenheten til skanneren direkte, uten en trådløs ruter.

Se følgende for mer informasjon.

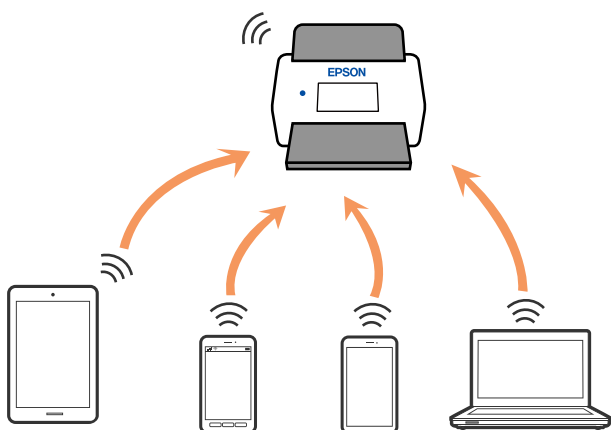
[“Koble til en smartenhet og skanner direkte \(Wi-Fi Direct\)” på side 23](#)

Koble til en smartenhet og skanner direkte (Wi-Fi Direct)

Wi-Fi Direct (Enkel AP) lar deg koble en smartenhet direkte til skanneren uten en trådløs ruter og skanne fra smartenheten.

Om Wi-Fi Direct


Bruk denne tilkoblingsmetoden når du ikke bruker Wi-Fi hjemme eller på kontoret, eller når du vil koble en datamaskin eller smartenhet direkte til skanneren. I denne modusen fungerer skanneren som en trådløs-ruter, og du kan koble enhetene til skanneren uten å bruke en vanlig trådløs-ruter. Enheter som er koblet direkte til skanneren kan imidlertid ikke kommunisere med hverandre gjennom skanneren.



Skanneren kan kobles til med Wi-Fi eller Ethernet og Wi-Fi Direct-modus (Enkel AP) samtidig. Hvis du starter en nettverkstilkobling i Wi-Fi Direct (Enkel AP)-modus mens skanneren er koblet til via Wi-Fi, blir imidlertid Wi-Fi midlertidig frakoblet.

Koble til en smartenhet med Wi-Fi Direct

Denne metoden gir deg mulighet til å koble skanneren direkte til smartenheter uten bruk av trådløs ruter.

1. Velg  på startskjermen.
2. Velg **Wi-Fi Direct**.
3. Velg **Start oppsett**.
4. Start Epson Smart Panel på smartenheten.
5. Følg instruksene som vises på Epson Smart Panel for å koble til skanneren din.
Når smartenheten din er koblet til skanneren kan du gå til neste trinn.
6. Velg **Ferdig** på skannerens kontrollpanel.

Koble fra Wi-Fi Direct (Enkel AP)-tilkobling

Det finnes to metoder for å deaktivere en Wi-Fi Direct (Enkel AP)-tilkobling: du kan deaktivere alle tilkoblinger ved hjelp av skannerens kontrollpanel eller deaktivere hver tilkobling fra datamaskinen eller smartenheten.

Når du vil deaktivere alle forbindelser, velger du  > **Wi-Fi Direct** > **Start oppsett** > **Endre** > **Deaktiver Wi-Fi Direct**.

Forsiktighetsregel:


Når Wi-Fi Direct (Enkel AP)-tilkobling deaktiveres, blir alle datamaskiner og smartenheter som er koblet til skanneren med Wi-Fi Direct (Enkel AP)-tilkobling frakoblet.

Merknad:

Hvis du vil koble fra en bestemt enhet, skal du koble den fra via enheten i stedet for via skanneren. Bruk en av følgende metoder til å koble Wi-Fi Direct (Enkel AP)-tilkoblingen fra enheten.

- Koble fra Wi-Fi-tilkoblingen til skannerens nettverksnavn (SSID).
- Koble til et annet nettverksnavn (SSID).

Endre innstillinger for Wi-Fi Direct (Enkel AP), som SSID

Når Wi-Fi Direct-tilkobling (Enkel AP) er aktivert, kan du endre innstillingene fra  > **Wi-Fi Direct** > **Start oppsett** > **Endre**, og så vil de følgende menyelementene vises.

Endre nettverksnavn

Endre Wi-Fi Direct (Enkel AP)-nettverksnavnet (SSID) brukt for å koble skanneren til ditt vilkårlige navn. Du kan angi nettverksnavnet (SSID) i ASCII-tegn som vises på programvaretastaturet på kontrollpanelet. Du kan skrive inn opptil 22 tegn.

Når nettverksnavnet (SSID) endres er alle tilkoblede enheter frakoblet. Bruk det nye nettverksnavnet (SSID) hvis du ønsker å koble til enheten igjen.

Endre passord

Endre Wi-Fi Direct-passordet (Enkel AP) for tilkobling til skanneren til din vilkårlige verdi. Du kan angi ASCII-tegn som vises på programvaretastaturet på kontrollpanelet. Du kan skrive inn 8 til 22 tegn.

Når passordet endres er alle tilkoblede enheter frakoblet. Bruk det nye passordet hvis du ønsker å koble til enheten igjen.

Endre frekvensområde

Endre frekvensområdet for Wi-Fi Direct som brukes til å koble til skanneren. Du kan velge 2,4 GHz eller 5 GHz.

Når frekvensområdet endres, blir alle tilkoblede enheter frakoblet. Koble til enheten på nytt.

Merk at når du endrer til 5 GHz, kan du ikke koble til enheter på nytt hvis enheten ikke støtter 5 GHz-frekvensområdet.

Innstillingen vises kanskje ikke, avhengige av området.

Deaktiver Wi-Fi Direct

Deaktiver Wi-Fi Direct-innstillingene for skanneren (Enkel AP). Når det deaktiveres, blir alle enheter koblet til skanneren i Wi-Fi Direct-tilkobling (Enkel AP), frakoblet.

Gjenopprett standardinnst.

Tilbakestill alle Wi-Fi Direct-innstillinger (Enkel AP) til standard.

Tilkoblingsinformasjonen for Wi-Fi Direct (Enkel AP) til smartenheten du lagret til skanneren er slettet.

Merknad:

Du kan også konfigurere fra **Nettverk-fanen > Wi-Fi Direct** på *Web Config* for følgende innstillinger.

Aktivere eller deaktivere Wi-Fi Direct (Enkel AP)

Endre nettverksnavn (SSID)

Endre passord

Endre frekvensområdet

Innstillingen vises kanskje ikke, avhengige av området.

Tilbakestille Wi-Fi Direct-innstillinger (Enkel AP)

Tilbakestille nettverkstilkoblingen

Dette avsnittet forklarer hvordan du foretar innstillingene for nettverkstilkobling og endrer tilkoblingsmetoden når du erstatter den trådløse ruterer eller datamaskinen.

Når du skifter ut den trådløse ruterer

Når du skifter ut den trådløse ruterer, angir du innstillinger for tilkoblingen mellom datamaskinen eller smartenheten og skanneren.

Du må angi disse innstillingene hvis du endrer Internett-leverandøren din og så videre.

Angi innstillinger for tilkobling til datamaskinen

Vi anbefaler å bruke installasjonsprogrammet for å koble skanneren til en datamaskin.

Åpne den følgende nettsiden og tast inn produktnavnet for å starte installasjonsprogrammet. Gå til **Oppsett**, og start konfigurasjonen.

<https://epson.sn>

Du kan se bruksanvisningene i Web-filmhåndbøker. Åpne følgende URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Velge tilkoblingsmetode

Følg instruksjonene på skjermen. På skjermbildet **Velg installasjonsalternativ** velger du **Sett opp Skriver-tilkobling på nytt (for ny nettverksruter eller endring av USB til nettverk osv.)**, og klikker deretter på **Neste**.

Følg instruksjonene på skjermen for å fullføre oppsettet.

Hvis du ikke kan koble til, kan du se følgende for å prøve å løse problemet.

[“Kan ikke koble til et nettverk” på side 32](#)

Angi innstillinger for tilkobling til smartenheten

Du kan bruke skanneren fra en smartenhet når du kobler skanneren til samme Wi-Fi-nettverk (SSID) som smartenheten. Åpne den følgende nettsiden og tast inn produktnavnet for å betjene skanneren fra en smartenhet. Gå til **Oppsett**, og start konfigurasjonen.

<https://epson.sn>

Åpne nettstedet fra smartenheten som du ønsker å koble til skanneren.

Når du endrer datamaskinen

Når du endrer datamaskinen, må du angi tilkoblingsinnstillinger mellom datamaskinen og skanneren.

Angi innstillinger for tilkobling til datamaskinen

Vi anbefaler å bruke installasjonsprogrammet for å koble skanneren til en datamaskin.

Åpne den følgende nettsiden og tast inn produktnavnet for å starte installasjonsprogrammet. Gå til **Oppsett**, og start konfigurasjonen.

<https://epson.sn>

Du kan se bruksanvisningene i Web-filmhåndbøker. Åpne følgende URL.

<https://support.epson.net/publist/vlink.php?code=NPD7509>

Følg instruksjonene på skjermen.

Endre tilkoblingsmetoden til datamaskinen

Dette avsnittet forklarer hvordan du endrer tilkoblingsmetoden når datamaskinen og skanneren er koblet til.

Endre nettverkstilkoblingen fra Ethernet til Wi-Fi

Endre Ethernet-tilkobling til Wi-Fi-tilkobling fra skannerens kontrollpanel. Metoden for å endre tilkoblingsmetode er essensielt den samme som metoden for endring av Wi-Fi-innstillinger.

Relatert informasjon

➔ [“Koble til trådløst LAN \(Wi-Fi\)” på side 19](#)

Endre nettverkstilkoblingen fra Wi-Fi til Ethernet

Følg trinnene nedenfor hvis du vil endre fra en Wi-Fi-tilkobling til en Ethernet-tilkobling.

1. Velg **Innst.** på startskjermen.
2. Velg **Nettverksinnstillinger > Oppsett av kablet LAN.**
3. Følg instruksjonene på skjermen.

Endre fra USB til en nettverkstilkobling

Bruke installasjonsprogrammet og konfigurere igjen med en annen tilkoblingsmetode.

Åpne den følgende nettsiden og tast inn produktnavnet. Gå til **Oppsett**, og start konfigurasjonen.

<https://epson.sn>

Velge Endre tilkoblingsmetodene

Følg instruksjonene i hvert vindu. På skjermbildet **Velg installasjonsalternativ** velger du **Sett opp Skriver-tilkobling på nytt (for ny nettverksruter eller endring av USB til nettverk osv.)**, og klikker deretter på **Neste**.

Velg nettverkstilkoblingen du vil bruke, **Koble via trådløst nettverk (Wi-Fi)** eller **Koble til via kablet LAN (Ethernet)**, og klikk deretter på **Neste**.

Følg instruksjonene på skjermen for å fullføre oppsettet.

Kontrollere statusen for nettverkstilkoblingen

Du kan sjekke tilkoblingsstatus for nettverket på følgende vis.

Kontrollere status for nettverkstilkoblingen fra kontrollpanelet

Du kan sjekke status for nettverkstilkobling med nettverksikonet eller nettverksinformasjonen på skannerens kontrollpanel.

Kontrollere status for nettverkstilkoblingen med nettverksikonet

Du kan kontrollere tilkoblingsstatus og styrken på radiobølgene ved hjelp av nettverksikonet på skannerens startskjerm.



	<p>Viser status for nettverkstilkobling.</p> <p>Velg ikonet for å kontrollere og endre gjeldende innstillinger. Dette er snarveien for følgende meny.</p> <p>Innst. > Nettverksinnstillinger > Wi-Fi-oppsett</p>
	<p>Skanneren er ikke tilkoblet et trådløst (Wi-Fi) nettverk.</p>
	<p>Skanneren søker etter SSID, IP-adresse med fjernet angivelse eller har problemer med et trådløst (Wi-Fi)-nettverk.</p>
	<p>Indikerer at skanneren er koblet til et trådløst nettverk (Wi-Fi).</p> <p>Antall streker indikerer signalstyrken på tilkoblingen. Jo flere streker det er, jo sterkere tilkobling.</p>
	<p>Skanneren er ikke koblet til et trådløst (Wi-Fi) nettverk i Wi-Fi Direct-modus (Enkel AP).</p>
	<p>Skanneren er koblet til et trådløst (Wi-Fi) nettverk i Wi-Fi Direct-modus (Enkel AP).</p>
	<p>Skanneren er ikke tilkoblet et kablet (Ethernet) nettverk eller fjernet angivelse av denne.</p>
	<p>Skanneren er tilkoblet et kablet (Ethernet) nettverk.</p>

Vise detaljert nettverksinformasjon på kontrollpanelet

Når skanneren er koblet til nettverket, kan du også vise annen nettverksrelatert informasjon ved å trykke nettverksmenyene du vil kontrollere.

1. Velg **Innst.** på startskjermen.
2. Velg **Nettverksinnstillinger > Nettverkstatus.**
3. For å kontrollere informasjonen, kan du velge menyene du vil kontrollere.
 - Status for kablet LAN/Wi-Fi
Viser nettverksinformasjon (enhetsnavn, tilkobling, signalstyrke, også videre) for Ethernet eller Wi-Fi-tilkobling.
 - Wi-Fi Direct-status
Viser hvorvidt Wi-Fi Direct er aktivert eller deaktivert, og SSID, passord også videre for Wi-Fi Direct-tilkoblinger.
 - E-postserverstatus
Viser nettverksinformasjonen til e-postserveren.

Nettverksspesifikasjoner

Wi-Fi-spesifikasjoner

Se følgende tabell for Wi-Fi-spesifikasjonene.

Land eller regioner utenom de som er oppført nedenfor	Tabell A
---	-----------------

Irland, Storbritannia, Østerrike, Tyskland, Liechtenstein, Sveits, Frankrike, Belgia, Luxemburg, Nederland, Italia, Portugal, Spania, Danmark, Finland, Norge, Sverige, Island, Kroatia, Kypros, Hellas, Nord-Makedonia, Serbia, Slovenia, Malta, Bosnia-Hercegovina, Kosovo, Montenegro, Albania, Bulgaria, Tsjekkia, Estland, Ungarn, Latvia, Litauen, Polen, Romania, Slovakia, Israel, Australia, New Zealand, Taiwan	Tabell B
Tyrkia	DS-900WN: Serienummer som begynner med XDA8: tabell A Serienummer som begynner med XDA7: tabell B
	DS-800WN: Serienummer som begynner med XDA2: tabell A Serienummer som begynner med XD9Z: tabell B

Tabell A

Standarder	IEEE 802.11b/g/n* ¹
Frekvensområde	2400–2483,5 MHz
Maksimal radiofrekvenskraft overført	20 dBm (EIRP)
Kanaler	1/2/3/4/5/6/7/8/9/10/11/12/13
Tilkoblingsmoduser	Infrastruktur, Wi-Fi Direct (Enkel AP)* ² * ³
Sikkerhetsprotokoller* ⁴	WEP (64/128bit), WPA2-PSK (AES)* ⁵ , WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Bare tilgjengelig for HT20

*2 Støttes ikke for IEEE 802.11b

*3 Infrastruktur- og Wi-Fi Direct-modus eller en Ethernet-tilkobling kan brukes samtidig.

*4 Wi-Fi Direct støtter kun WPA2-PSK (AES).

*5 Overholder WPA2-standarder med støtte for WPA/WPA2 Personal.

Tabell B

Standarder	IEEE 802.11a/b/g/n* ¹ /ac
Frekvensområder	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz

Kanaler	Wi-Fi	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12* ² /13* ²
		5 GHz* ³	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12* ² /13* ²
		5 GHz* ³	W52 (36/40/44/48) W58 (149/153/157/161/165)
Tilkoblingsmoduser	Infrastruktur, Wi-Fi Direct (enkelt tilgangspunkt)* ⁴ , * ⁵		
Sikkerhetsprotokoller* ⁶	WEP (64/128bit), WPA2-PSK (AES)* ⁷ , WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Bare tilgjengelig for HT20

*2 Ikke tilgjengelig i Taiwan

*3 Tilgjengeligheten til disse kanalene og bruken av produktene utendørs med disse kanalene varierer etter sted. Les <http://support.epson.net/wifi5ghz/> for å få mer informasjon

*4 Støttes ikke for IEEE 802.11b.

*5 Infrastruktur- og Wi-Fi Direct-modus eller en Ethernet-tilkobling kan brukes samtidig.

*6 Wi-Fi Direct støtter bare WPA2-PSK (AES).

*7 Overholder WPA2-standarder med støtte for WPA/WPA2 Personal.

Ethernet-spesifikasjoner

Standarder	IEEE802.3i (10BASE-T)* ¹ IEEE802.3u (100BASE-TX)* ¹ IEEE802.3ab (1000BASE-T)* ¹ IEEE802.3az (Energi Effektivt Ethernet)* ²
Kommunikasjonsmodus	Auto, 10 Mbps Fulldupleks, 10 Mbps Halvdupleks, 100 Mbps Fulldupleks, 100 Mbps Halvdupleks
Kontakt	RJ-45

*1 Bruk en kategori 5e eller høyere STP (skjermet tvunnet par) kabel for å forhindre fare for radioforstyrrelser.

*2 Den tilkoblede enheten skal oppfylle IEEE802.3az standarder.

Nettverksfunksjoner og støtte for IPv4/IPv6

Funksjoner	Støttes
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4

Sikkerhetsprotokoll

IEEE802.1X*	
IPsec/IP Filtering	
SSL/TLS	HTTPS Server/Client
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Du må bruke en tilkoblingsenhet som oppfyller IEEE802.1X.

Bruke porten for skanneren

Skanneren bruker følgende port. Disse portene bør tillates å bli gjort tilgjengelig av nettverksadministrator etter behov.

Når senderen (klienten) er skanneren

Bruk	Destinasjon (server)	Protokoll	Portnummer	
Filsending (når skann til nettverksmappe brukes fra skanneren)	FTP/FTPS-server	FTP/FTPS (TCP)	20	
			21	
	Filsriver	SMB (TCP)	445	
			NetBIOS (UDP)	137
				138
	WebDAV-server	NetBIOS (TCP)	139	
Protocol HTTP (TCP)			80	
		Protocol HTTPS (TCP)	443	
E-postsending (når skann til e-post-funksjonen brukes fra skanneren)	SMTP-server	SMTP (TCP)	25	
		SMTP SSL/TLS (TCP)	465	
		SMTP STARTTLS (TCP)	587	
POP før SMTP-tilkobling (når skann til e-post-funksjonen brukes fra skanneren)	POP-server	POP3 (TCP)	110	
Når Epson Connect er brukt	Epson Connect-server	HTTPS	443	
		XMPP	5222	
Samler brukerinformasjon (bruk kontaktene fra skanneren)	LDAP-server	LDAP (TCP)	389	
		LDAP SSL/TLS (TCP)	636	
		LDAP STARTTLS (TCP)	389	

Bruk	Destinasjon (server)	Protokoll	Portnummer
Brukergodkjenning når brukerinformasjon samles inn (når kontaktene fra skanneren brukes) Brukergodkjenning når du bruker skann til nettverksmappe (SMB) fra skanneren	KDC-server	Kerberos	88
Control WSD	Klientdatamaskin	WSD (TCP)	5357
Søk på datamaskinen ved push-skanning fra en applikasjon	Klientdatamaskin	Registrering av nettverkspush-skann	2968

Når senderen (klienten) er klientdatamaskinen

Bruk	Destinasjon (server)	Protokoll	Portnummer
Registrer skanneren fra et program som EpsonNet Config og skannerdriveren.	Skanner	ENPC (UDP)	3289
Samle og konfigurere MIB-informasjon fra et program som EpsonNet Config og skannerdriver.	Skanner	SNMP (UDP)	161
Søker WSD-skanner	Skanner	WS-Discovery (UDP)	3702
Videreseng skannedataene fra en applikasjon	Skanner	Nettverksskann (TCP)	1865
Henter jobbinformasjon ved push-skanning fra en applikasjon	Skanner	Nettverkspush-skann	2968
Web Config		HTTP (TCP)	80
		HTTPS (TCP)	443

Problemløsning

Kan ikke koble til et nettverk

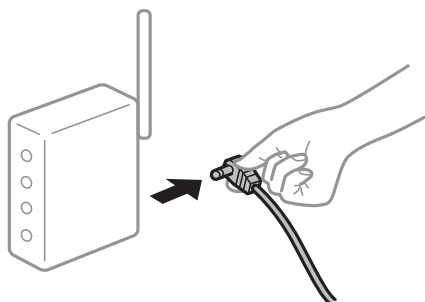
Problemet kan være ett av følgende problemer.

■ Noe gikk galt med nettverksenheten for Wi-Fi-tilkobling.

Løsninger

Slå av enhetene du vil koble til nettverket. Vent i omtrent 10 sekunder og slå deretter på enhetene i følgende rekkefølge: trådløse ruter, datamaskin eller smartenhet og deretter skanneren. Flytt skanneren og

datamaskinen eller smartenheten nærmere den trådløse ruterer for å bedre radiobølgekommunikasjonen og prøv å angi nettverksinnstillinger på nytt.



Enhetene kan ikke motta signaler fra den trådløse ruterer fordi de er for langt fra hverandre.

Løsninger

Når du har flyttet datamaskinen eller smartenheten og skanneren nærmere den trådløse ruterer, slår du av den trådløse ruterer, og slår den deretter på igjen.

Når du endrer den trådløse ruterer, stemmer ikke innstillingene med den nye ruterer.

Løsninger

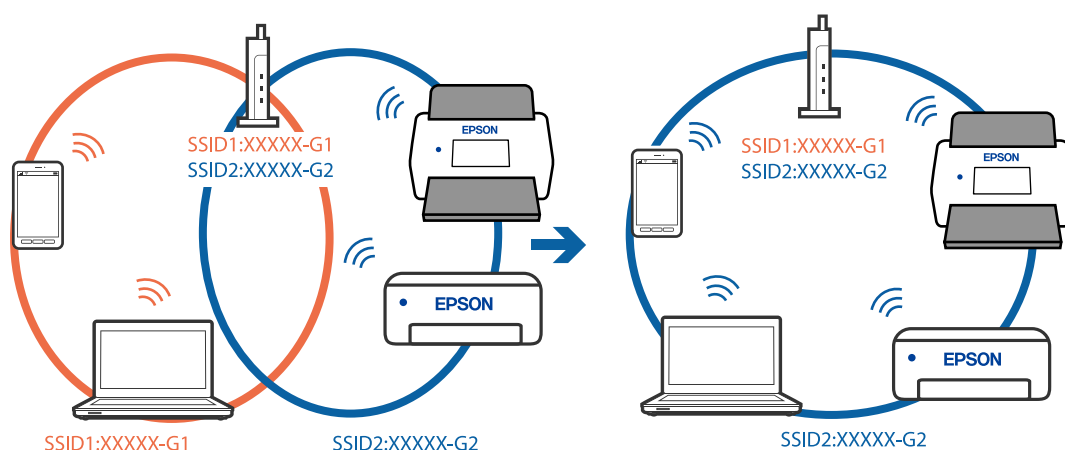
Gjør tilkoblingsinnstillingene på nytt slik at de samsvarer med den nye trådløse ruterer.

SSID-ene som er koblet fra datamaskinen eller smartenhet og datamaskin, er forskjellige.

Løsninger

Når du bruker flere trådløse rutere samtidig, eller den trådløse ruterer har flere SSID-er, og enhetene er koblet til forskjellige SSID-er, kan du ikke koble til den trådløse ruterer.

Koble datamaskinen eller smartenheten til samme SSID som skanneren.



En skillefunksjon for personvern er tilgjengelig på den trådløse ruterer.

Løsninger

De fleste trådløse rutere har en skillefunksjon for personvern som blokkerer kommunikasjon mellom enhetene. Hvis du ikke kan kommunisere mellom skanneren og datamaskinen eller smartenheten, selv om de er koblet til samme nettverk, kan du deaktivere skillefunksjonen for personvern på den trådløse ruterer. Se bruksanvisningen som følger med den trådløse ruterer for mer informasjon.

IP-adressen er ikke tilordnet på riktig måte.

Løsninger

Hvis IP-adressen som er tilordnet til skanneren er 169.254.XXX.XXX, og nettverksmasken er 255.255.0.0, kan ikke IP-adressen tilordnes på riktig måte.

Velg **Innst.** > **Nettverksinnstillinger** > **Avansert** > **TCP/IP-oppsett** på skannerens kontrollpanel, og kontroller deretter IP-adressen og nettmasken tilordnet skanneren.

Start den trådløse ruteren på nytt eller tilbakestill skannerens nettverksinnstillinger.

Det er et problem med nettverksinnstillingene på datamaskinen.

Løsninger

Prøv å åpne hvilken som helst nettside fra datamaskinen for å sørge for at datamaskinens nettverksinnstillinger er riktige. Hvis du ikke kan åpne noen nettsider, er det et problem på datamaskinen.

Kontroller nettverkstilkoblingen på datamaskinen. Se i dokumentasjonen som fulgte med datamaskinen for nærmere informasjon.

Skanneren er koblet til Ethernet ved hjelp av enheter som støtter IEEE 802.3az (energieffektivt Ethernet).

Løsninger

Når du kobler til skanneren med Ethernet ved hjelp av enheter som støtter IEEE 802.3az (energieffektivt Ethernet), kan følgende problemer oppstå avhengig av huben eller ruter du bruker.

- Tilkoblingen blir ustabil, skanneren kobler seg til og fra igjen og igjen.
- Kan ikke koble til skanneren.
- Kommunikasjonshastigheten blir sakte.

Følg trinnene under for å deaktivere IEEE 802.3az for skanneren og deretter koble til.

1. Ta ut Ethernet-kabelen som er koblet til datamaskinen og skanneren.
2. Når IEEE 802.3az for datamaskinen er aktivert, deaktiverer du det.
Se i dokumentasjonen som fulgte med datamaskinen for nærmere informasjon.
3. Koble sammen datamaskinen og skanneren direkte med en Ethernet-kabel.
4. Sjekk nettverksinnstillingene på skanneren.
Velg **Innst.** > **Nettverksinnstillinger** > **Nettverkstatus** > **Status for kablet LAN/Wi-Fi**.
5. Kontroller skannerens IP-adresse.
6. Åpne Web Config på datamaskinen.
Start en nettleser og angi skannerens IP-adresse.
["Slik kjører du Web Config i en nettleser"](#) på side 37
7. Velg **Nettverk**-fanen > **Kablet lokalnett**.
8. Velg **Av** ved **IEEE 802.3az**.

9. Klikk på **Neste**.
10. Klikk på **OK**.
11. Ta ut Ethernet-kabelen som er koblet til datamaskinen og skanneren.
12. Hvis du deaktiverte IEEE 802.3az for datamaskinen i trinn 2, aktiverer du det.
13. Koble Ethernet-kablene som du fjernet i trinn 1 til datamaskinen og skanneren.
Hvis problemet vedvarer, kan det hende at andre enheter enn skanneren forårsaker problemet.

■ Skanneren er slått av.

Løsninger

Pass på at skanneren er slått på.

Du må også vente til statuslampen slutter å blinke, noe som indikerer at skanneren er klar til å skanne.

Programvare for å konfigurere skanneren

Program for konfigurering av skanneoperasjoner (Web Config)37
Epson Device Admin.38

Program for konfigurering av skanneoperasjoner (Web Config)

Web Config er et program som kjøres i nettlesere, for eksempel Microsoft Edge og Safari, på en datamaskin eller smartenhet. Du kan bekrefte skannerens status eller endre nettverkstjenesten og skanneinnstillingene. Koble skanneren og datamaskinen eller enheten til det samme nettverket for å bruke Web Config.

Følgende nettlesere støttes. Bruk kun den siste versjonen.

Microsoft Edge, Windows Internet Explorer, Firefox, Chrome, Safari

Merknad:

Du kan bli bedt om å angi administratorpassordet mens du bruker denne enheten. Se følgende for mer informasjon om administratorpassord.

“Merknader om administratorpassordet” på side 10

Relatert informasjon

➔ [“Får ikke tilgang til Web Config” på side 63](#)

Slik kjører du Web Config i en nettleser

Skanneren kommer med en innebygget programvare kalt Web Config (en nettside der du kan angi innstillinger). For å åpne Web Config skriver du inn IP-adressen til en nettverkstilkoblet skanner i nettleseren din.

1. Kontroller skannerens IP-adresse.

Velg **Innst.** > **Nettverksinnstillinger** > **Nettverkstatus** på skannerens kontrollpanel. Velg deretter den aktive tilkoblingsmetoden (**Status for kablet LAN/Wi-Fi** eller **Wi-Fi Direct-status**) for å bekrefte skannerens IP-adresse.

Eksempel på IP-adresse: 192.168.100.201

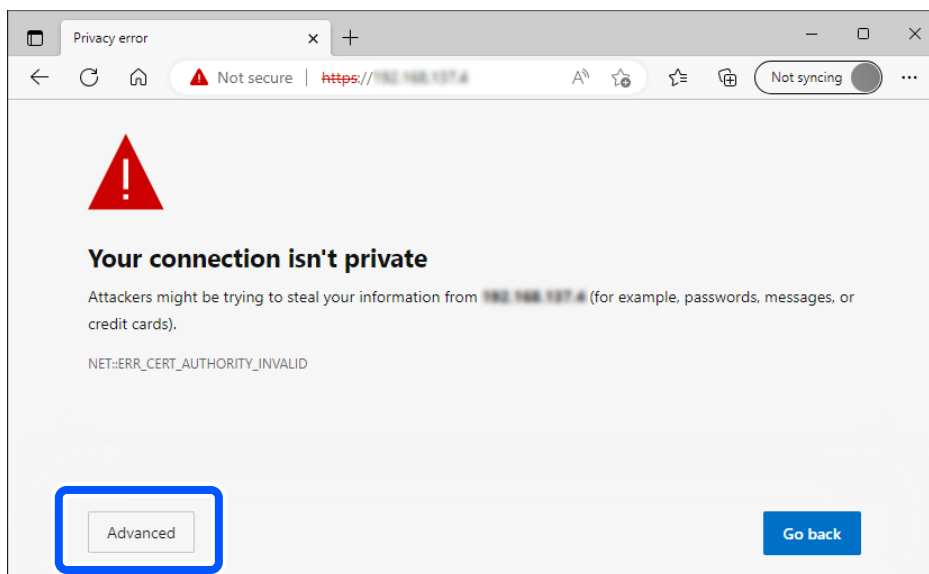
2. Start en nettleser fra en datamaskin eller en smartenhet, og skriv deretter inn skannerens IP-adresse i adresselinjen.

Format: `http://skannerens IP-adresse/`

Eksempel: `http://192.168.100.201/`

Hvis advarselskjermen vises i nettleseren din, kan du trygt ignorere advarselen og vise nettsiden (Web Config). Siden skanneren bruker et selvsignert sertifikat når HTTPS åpnes, vises en advarsel i nettleseren når du starter Web Config. Dette indikerer ikke noe problem og kan trygt ignoreres. Avhengig av nettleseren må du kanskje klikke på **Avanserte innstillinger** for å se nettsiden.

Eksempel: for Microsoft Edge



Merknad:

Hvis advarselskjermen ikke vises, gå videre til neste trinn.

Bruk følgende format for IPv6-adresser.

Format: `http://[skannerens IP-adresse]/`

Eksempel: `http://[2001:db8::1000:1]/`

3. For å endre skannerinnstillingene må du logge på som Web Config-administrator.

Klikk på **logg på** øverst til høyre på skjermen. Skriv inn **Brukernavn** og **Nåværende passord**, og klikk deretter på **OK**.

Følgende gir opprinnelige verdier for Web Config-administratorinformasjon.

·Brukernavn: ingen (tomt)

·Passord: avhenger av etiketten på produktet.

Hvis det er en PASSWORD-etikett på baksiden, angir du det 8-sifrede nummeret på etiketten. Hvis det ikke er en PASSWORD-etikett der, angir du serienummeret på etiketten på baksiden av produktet som administratorpassord den første gangen.

Merknad:

Hvis **logg av** vises øverst til høyre på skjermen er du allerede logget inn som administrator.

Du logges av automatisk etter ca. 20 minutter med inaktivitet.

Epson Device Admin

Epson Device Admin er et flerfunksjonelt program som lar deg administrere enhetene på et nettverk.

Du kan bruke konfigurasjonsmaler til å bruke forente innstillinger på flere skannere på et nettverk. Dette gjør at det egner seg til å installere og administrere flere skannere.

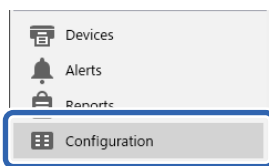
Du kan laste ned Epson Device Admin fra Epsons nettsted for kundestøtte. For mer informasjon om hvordan du bruker dette programmet, kan du se hjelpedokumentasjonen for Epson Device Admin.

Konfigurasjonsmal

Opprette konfigurasjonsmal

Opprette ny konfigurasjonsmal.

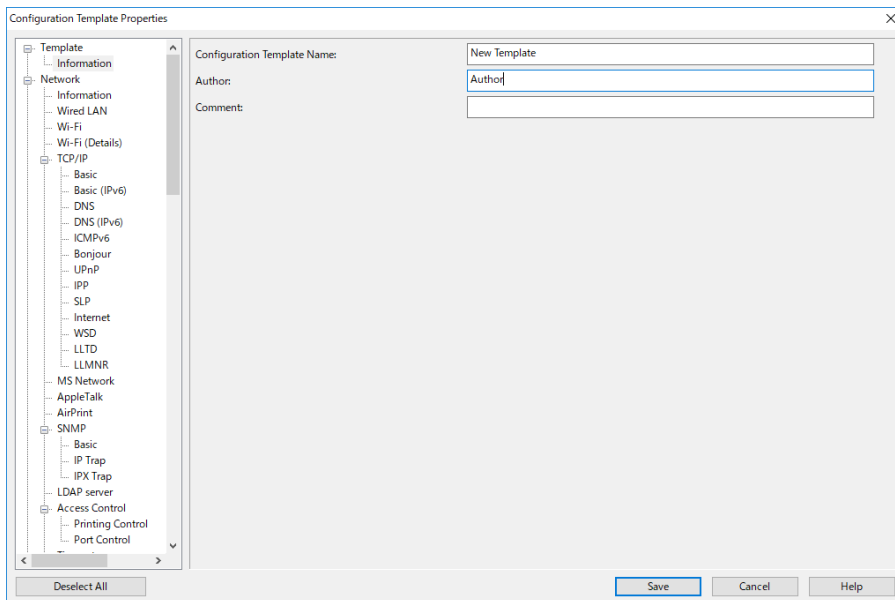
1. Start Epson Device Admin.
2. Velg **Configuration** på sidestolpen med oppgavemeny.



3. Velg **New** på båndmenyen.



4. Angi alle elementene.



Artikkel	Forklaring
Configuration Template Name	Navn på konfigurasjonsmal. Skriv inn opptil 1024 tegn i Unicode (UTF-8).
Author	Informasjon om skaperen av malen. Skriv inn opptil 1024 tegn i Unicode (UTF-8).

Artikkel	Forklaring
Comment	Angi valgfri informasjon. Skriv inn opptil 1024 tegn i Unicode (UTF-8).

5. Velg elementene du ønsker å angi til venstre.

Merknad:

Klikk på menyelementene til venstre for å bytte til hvert skjermbilde. Angitt verdi beholdes dersom du bytter skjermbilde, men ikke hvis du avbryter det. Når du er ferdig med alle innstillingene, klikk **Save**.

Bruke konfigurasjonsmal

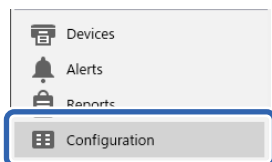
Bruke den lagrede konfigurasjonsmalen på skanneren. Det valgte elementet på malen brukes. Hvis målskanneren ikke har en egnet funksjon, brukes ikke dette.

Merknad:

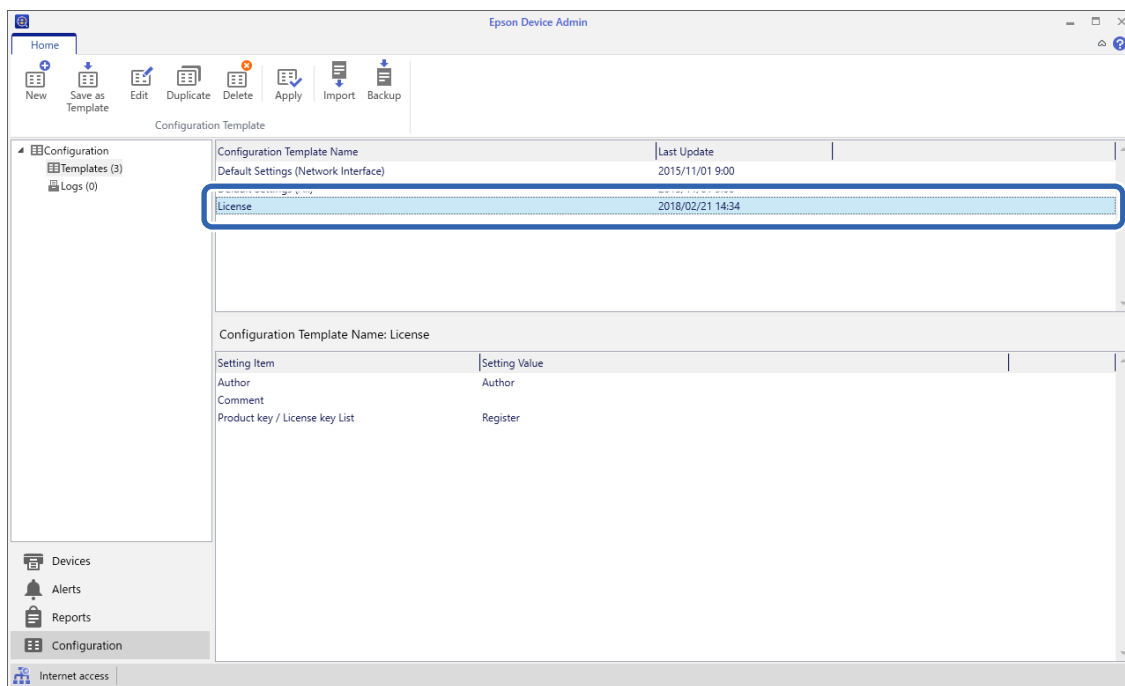
Når et administratorpassord er angitt for skanneren, må passordet konfigureres på forhånd.

1. Velg **Options** > **Password manager** fra båndmenyen på Enhetsliste-skjermbildet.
2. Velg **Enable automatic password management** og klikk så **Password manager**.
3. Velg riktig skanner, og klikk på **Edit**.
4. Angi passordet og klikk **OK**.

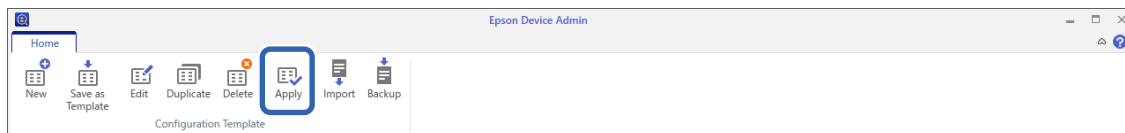
1. Velg **Configuration** på sidestolpen med oppgavemeny.



2. Velg konfigurasjonsmalen du ønsker å bruke **Configuration Template Name**.



3. Klikk **Apply** på båndmenyen.
Skjermbildet for enhetsvalg vises.

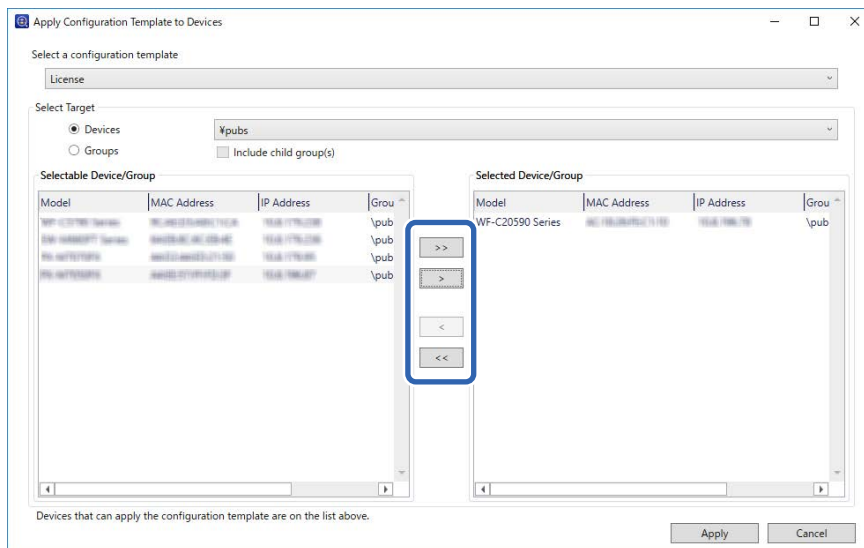


4. Velg konfigurasjonsmalen du vil bruke.

Merknad:

- Når du velger **Devices** og grupper som inneholder enheter fra rullegardinmenyen, vises hver enkelt enhet.
- Grupper vises når du velger **Groups**. Velg **Include child group(s)** hvis du ønsker å automatisk velge barnegrupper i den valgte gruppen.

5. Flytt skanneren eller gruppene du vil bruke malen for, til **Selected Device/Group**.



6. Klikk på **Apply**.
Det vises et bekreftelsesskjerm bilde for konfigurasjonsmalen som skal brukes.
7. Klikk på **OK** for å bruke konfigurasjonsmalen.
8. Når det vises en melding om at prosedyren er fullført, kan du klikke på **OK**.
9. Klikk **Details** og kontroller informasjonen.
Når vises på elementene du har brukt, har anvendelsen blitt utført.
10. Klikk på **Close**.

Nødvendige innstillinger for skanning

Registrere en e-postserver.	44
Opprette en nettverksmappe.	46
Gjøre kontakter tilgjengelig.	53
Konfigurere AirPrint.	62
Problemer ved forberedelse av nettverksskanning.	63

Registrere en e-postserver

Kontroller følgende før du konfigurerer e-postserveren.

Skanneren er koblet til nettverket

Innstillingsinformasjon for e-postserver

Når du bruker en internettbasert e-postserver, må du sjekke innstillingsinformasjonen fra leverandøren eller nettstedet.

Slik registrerer du

Åpne Web Config og velg **Nettverk**-fanen > **E-postserver** > **Grunnleggende**.

[“Slik kjører du Web Config i en nettleser” på side 37](#)

Du kan også angi innstillinger for skannerens kontrollpanel. Velg **Innst.** > **Nettverksinnstillinger** > **Avansert** > **E-postserver** > **Serverinnstillinger**.

Innstillingselementer for e-postserver

Element	Innstillinger og forklaring	
Godkjenningsmetode	Angi godkjenningsmetoden for skanneren som skal få tilgang til e-postserveren.	
	Av	Autentisering er deaktivert under kommunikasjon med en e-postserver.
	SMTP-autentisering	E-postserveren må støtte SMTP-godkjenning.
	POP før SMTP	Angi en POP3-server når du velger dette elementet.
Godkjent konto	Hvis du velger SMTP-autentisering eller POP før SMTP som Godkjenningsmetode , må du oppgi det autentiserte kontonavnet. Skriv inn mellom 0 og 255 tegn i ASCII (0x20–0x7E).	
Godkjent passord	Hvis du velger SMTP-autentisering eller POP før SMTP som Godkjenningsmetode , må du oppgi det autentiserte passordet. Skriv inn mellom 0 og 20 tegn i ASCII (0x20–0x7E).	
Avsenderens e-postadresse	Angi e-postadressen som skal brukes til å sende e-poster fra skanneren. Selv om du kan bruke en eksisterende e-postadresse, anbefaler vi at du skaffer og konfigurerer en dedikert e-postadresse slik at den kan skilles fra e-poster som sendes fra skanneren. Skriv inn opptil 255 tegn i ASCII (0x20–0x7E), bortsett fra : () < > [] ; ¥. Det første tegnet kan ikke være et punktum «.».	
SMTP-server adresse	Skriv inn mellom 0 og 255 tegn ved hjelp av A–Z a–z 0–9 . - . Du kan bruke IPv4- eller FQDN-format.	
SMTP-server portnummer	Skriv inn et tall mellom 1 og 65535.	
Sikker forbindelse	Spesifiser sikker tilkobling metode for e-postserveren.	
	Ingen	Hvis du velger POP før SMTP i Godkjenningsmetode , blir tilkoblingsmetoden satt til Ingen .
	SSL/TLS	Dette er tilgjengelig når Godkjenningsmetode er satt til Av eller SMTP-autentisering .
	STARTTLS	Dette er tilgjengelig når Godkjenningsmetode er satt til Av eller SMTP-autentisering .
Sertifikatvalidering (kun Web Config)	Sertifikatet er validert når dette er aktivert. Vi anbefaler å stille dette inn til Aktiver når Sikker forbindelse er angitt som noe annet enn Ingen .	

Element	Innstillinger og forklaring
POP3-server adresse	Hvis du velger POP før SMTP som Godkjenning metode , skriver du inn server-adressen til POP3-serveren. Du kan skrive inn mellom 0 og 255 tegn ved hjelp av A-Z a-z 0-9 . Du kan bruke IPv4- eller FQDN-format.
POP3-server portnummer	Når du velger, sett POP før SMTP i Godkjenning metode . Skriv inn et tall mellom 1 og 65535.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Kontrollere tilkoblingen til en e-postserver

1. Velg tilkoblingstest-menyen.

Når du konfigurerer fra Web Config:

Velg **Nettverk**-fanen > **E-postserver** > **Tilkoblingstest** > **Start**.

Når du gjør innstillinger fra kontrollpanelet:

Velg **Innst.** > **Nettverksinnstillinger** > **Avansert** > **E-postserver** > **Tilkoblingskontroll**.

Tilkoblingstesten til e-postserveren startes.

2. Sjekk testresultatet.

Testen er vellykket når du ser meldingen **Tilkoblingstesten var vellykket..**

Hvis det vises en feil, må du følge instruksene i meldingen for å løse feilen.

[“Testreferanser for e-postservertilkobling” på side 45](#)

Testreferanser for e-postservertilkobling

Melding	Årsak
SMTP-serverkommunikasjonsfeil. Kontroller følgende. - Nettverksinnstillinger	Denne meldingen vises når <ul style="list-style-type: none"> <input type="checkbox"/> Skanneren er ikke koblet til et nettverk <input type="checkbox"/> SMTP-serveren er nede <input type="checkbox"/> Nettverkstilkobling er frakoblet under kommunikasjon <input type="checkbox"/> Mottok ufullstendige data
POP3-serverkommunikasjonsfeil. Kontroller følgende. - Nettverksinnstillinger	Denne meldingen vises når <ul style="list-style-type: none"> <input type="checkbox"/> Skanneren er ikke koblet til et nettverk <input type="checkbox"/> POP3-serveren er nede <input type="checkbox"/> Nettverkstilkobling er frakoblet under kommunikasjon <input type="checkbox"/> Mottok ufullstendige data
Det oppstod en feil under tilkobling til SMTP-serveren. Kontroller følgende. - SMTP-serveradresse - DNS-server	Denne meldingen vises når <ul style="list-style-type: none"> <input type="checkbox"/> Tilkobling til en DNS-server mislyktes <input type="checkbox"/> Navnløsning for en SMTP-server mislyktes

Melding	Årsak
Det oppstod en feil under tilkobling til POP3-serveren. Kontroller følgende. - POP3-serveradresse - DNS-server	Denne meldingen vises når <ul style="list-style-type: none"> <input type="checkbox"/> Tilkobling til en DNS-server mislyktes <input type="checkbox"/> Navnløsning for en POP3-server mislyktes
SMTP-serverautentiseringfeil. Kontroller følgende. - Autentiseringsmetode - Autentisert konto - Autentisert passord	Denne meldingen vises når SMTP-serverautentisering mislyktes.
POP3-serverautentiseringfeil. Kontroller følgende. - Autentiseringsmetode - Autentisert konto - Autentisert passord	Denne meldingen vises når POP3-serverautentisering mislyktes.
Kommunikasjonsmetode støttes ikke. Kontroller følgende. - SMTP-serveradresse - SMTP-serverportnummer	Denne meldingen vises når du prøver å kommunisere med ikke-støttede protokoller.
Tilkobling til SMTP-serveren mislyktes. Endre Sikker forbindelse til Ingen.	Denne meldingen vises når SMTP ikke samsvarer mellom en server og en klient eller når serveren ikke støtter sikker SMTP-tilkobling (SSL-tilkobling).
Tilkobling til SMTP-serveren mislyktes. Endre Sikker forbindelse til SSL/TLS.	Denne meldingen vises når det oppstår en SMTP uoverensstemmelse mellom en server og en klient, eller når serveren forespør om å bruke en SSL/TLS tilkobling for en SMTP sikker forbindelse.
Tilkobling til SMTP-serveren mislyktes. Endre Sikker forbindelse til STARTTLS.	Denne meldingen vises når det oppstår en SMTP uoverensstemmelse mellom en server og en klient, eller når serveren forespør om å bruke en STARTTLS tilkobling for en SMTP sikker forbindelse.
Tilkoblingen er ikke klarert. Kontroller følgende. - Dato og klokkeslett	Denne meldingen vises når skannerens dato og klokkeslett er feil eller sertifikatet er utløpt.
Tilkoblingen er ikke klarert. Kontroller følgende. - CA-sertifikat	Denne meldingen vises når skanneren ikke har et rotsertifikat som tilsvarende serveren eller en CA-sertifikat ikke har blitt importert.
Tilkoblingen er ikke sikret.	Denne meldingen vises når det fremstilte sertifikatet er skadet.
SMTP-serverautentisering mislyktes. Endre autentiseringsmetode til SMTP-AUTH.	Denne meldingen vises når en uoverensstemmelse for autentiseringsmetode oppstår mellom en server og en klient. Serveren støtter SMTP-autentisering.
SMTP-serverautentisering mislyktes. Endre autentiseringsmetode til POP før SMTP.	Denne meldingen vises når en uoverensstemmelse for autentiseringsmetode oppstår mellom en server og en klient. Serveren støtter ikke SMTP-autentisering.
Avsenderens e-postadresse er feil. Endre til e-postadressen for e-posttjenesten.	Denne meldingen vises når den angitte avsenderens e-postadresse er feil.
Får ikke tilgang til produktet før behandlingen er fullført.	Denne meldingen vises når skanneren er opptatt.

Opprette en nettverksmappe

Opprette en nettverksmappe på datamaskinen. Datamaskinen må være koblet til samme nettverk som skanneren.


Metoden for å angi en nettverksmappe varierer avhengig av miljø. Dette er et eksempel på å opprette en nettverksmappe på skrivebordet til en datamaskin i følgende miljø.

- Operativsystem: Windows 10
- Hvor opprettes den delte mappen: skrivebord
- Mappebane: C:\Users\xxxx\Desktop\scan_folder (opprett en nettverksmappe kalt «scan_folder» på skrivebordet)

1. Logg inn på datamaskinen du vil opprette en nettverksmappe på, med en brukerkonto som har administratortillatelser.

Merknad:

Hvis du ikke vet hvilken brukerkonto som har administratortillatelser, kan du spørre dataadministratoren.

2. Sørg for at enhetsnavnet (datamaskinnavn) ikke inneholder dobbelbyte-tegn. Klikk på Windows Start-knappen, og velg deretter  **Innstillinger > System > Om.**

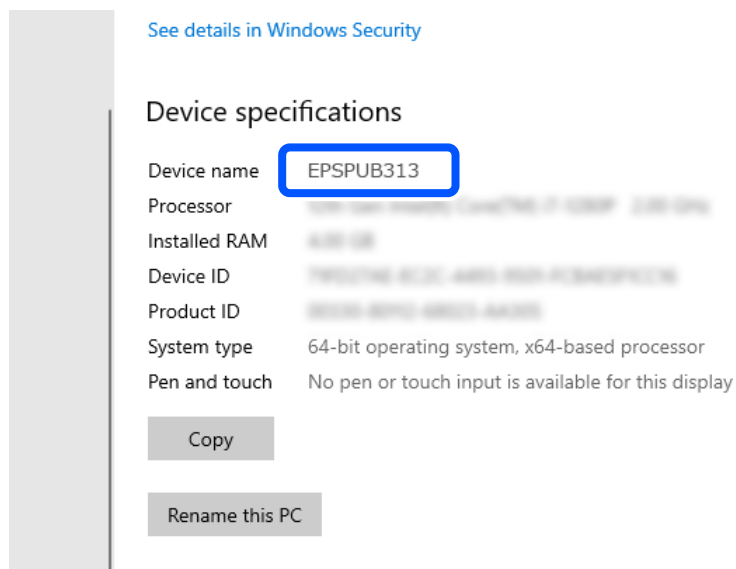
Merknad:

Hvis det er dobbelbyte-tegn i enhetsnavnet, kan lagringen av filen mislykkes.

3. Sjekk om strengen som er vist i **Enhetsspesifikasjoner > Enhetsnavn** ikke inneholder dobbelbyte-tegn.

Det skal ikke oppstå problemer så lenge navnet kun inneholder enkeltbyte-tegn. Lukk skjermen.

Eksempel: EPSPUB313



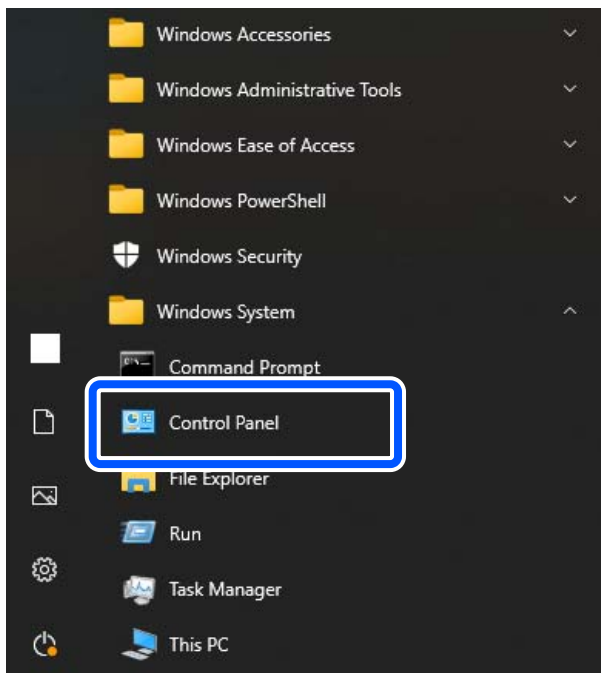
Forsiktighetsregel:

Hvis enhetsnavnet inneholder dobbelbyte-tegn, må du bruke en datamaskin som ikke bruker dobbelbyte-tegn eller gi enheten et nytt navn.

Hvis du må endre enhetsnavnet, må du sørge for å få tillatelse fra dataadministratoren på forhånd da dette kan påvirke dataadministrasjon og tilgang til ressurser.

Sjekk deretter datamaskininnstillingene.

4. Klikk på Windows Start-knappen og velg **Windows-system > Kontrollpanel**.



5. Klikk på **Nettverk og Internett** på kontrollpanelet > **Nettverks- og delingscenter > Endre avanserte deleinnstillinger**.

Nettverksprofilen vises.

6. Sørg for at **Slå på fil- og skriverdeling** er valgt under **Fil- og skriverdeling** for nettverksprofilen (aktiv profil).

Hvis dette allerede er valgt, klikker du **Avbryt** og lukker vinduet.

Når du endrer innstillingene, klikk **Lagre endringer** og lukk vinduet.

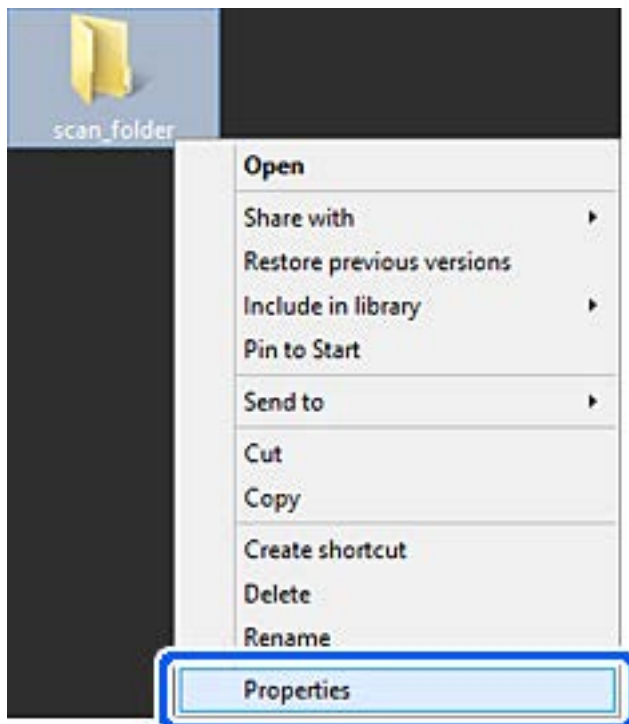
Opprett deretter en nettverksmappe.

7. Opprett en mappe på skrivebordet og gi den navn.

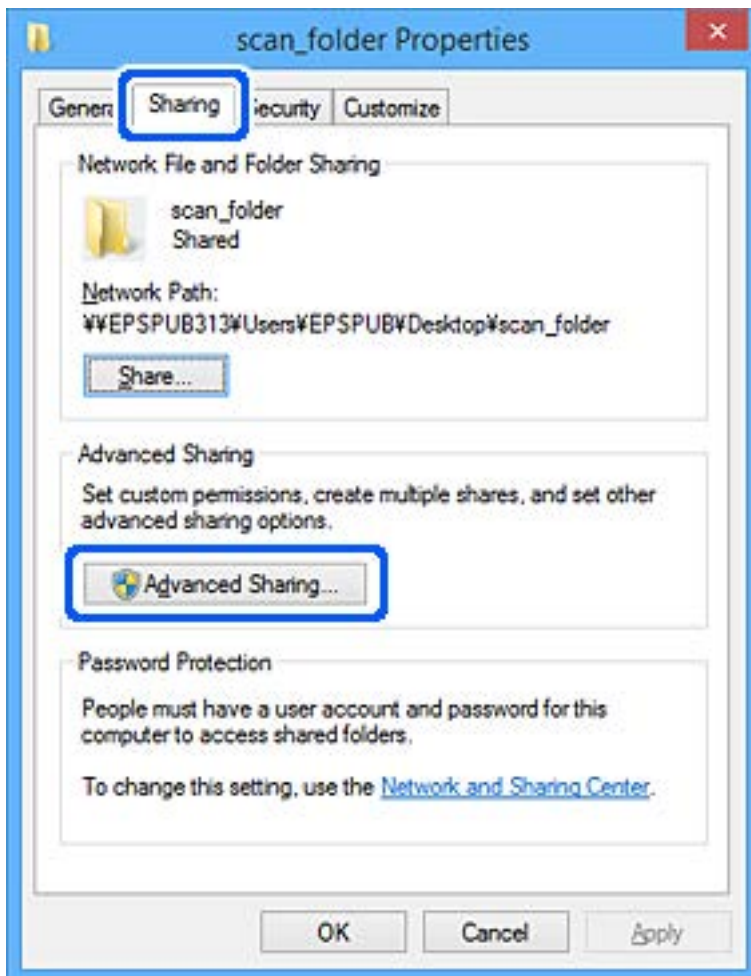
Skriv mellom 1 og 12 alfanumeriske tegn for mappenavnet. Hvis mappenavnet er lenger enn 12 tegn kan det hende at du ikke har tilgang på mappen, dette avhenger av miljøet.

Eksempel: scan_folder

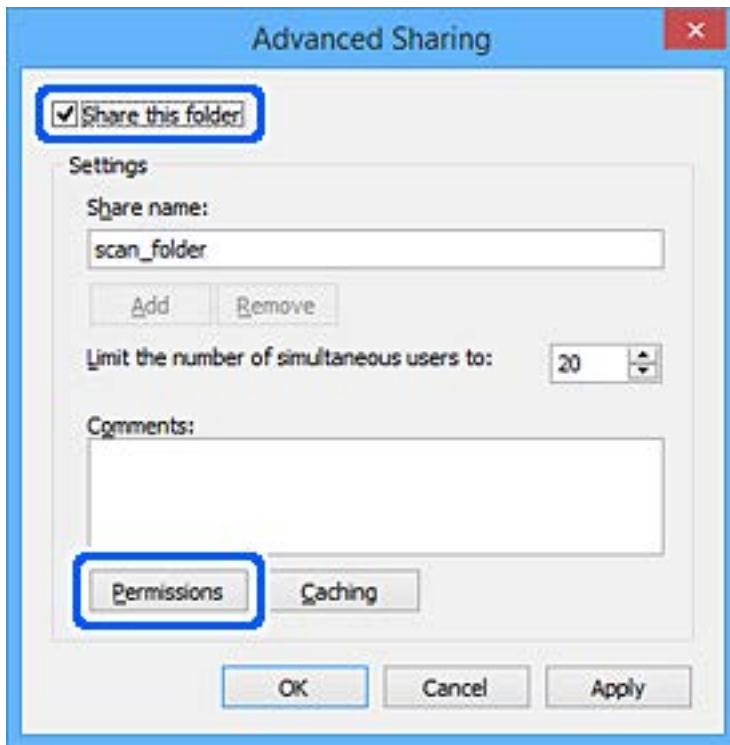
8. Høyreklikk på mappen og velg deretter **Egenskaper**.



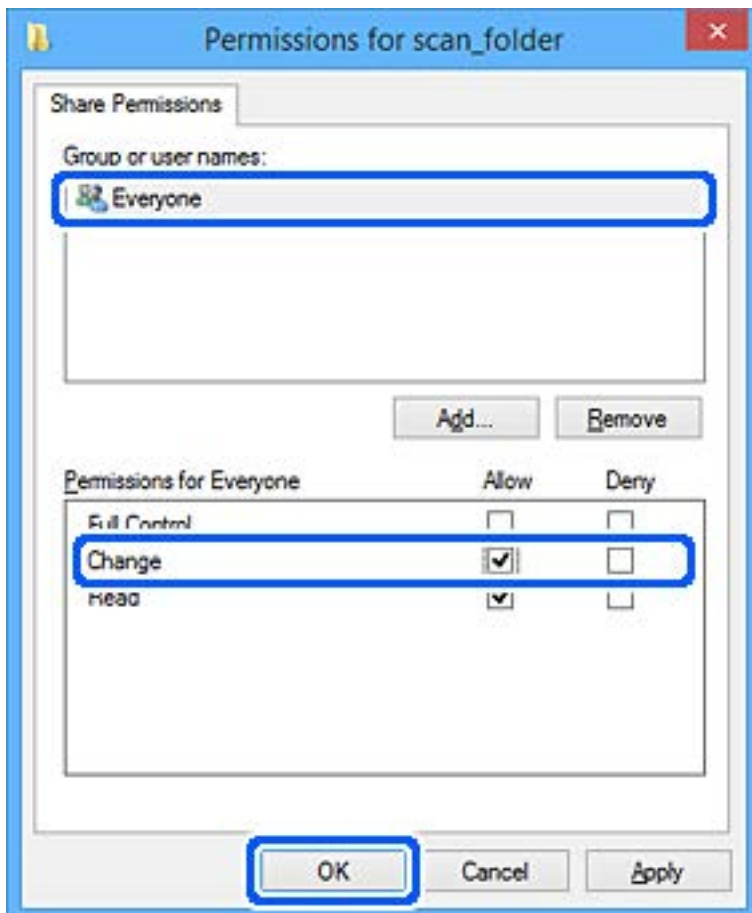
9. Klikk på **Avansert deling** på **Deling**-fanen.



10. Velg **Del denne mappen** og klikk deretter **Tillatelser**.



11. Velg **Alle** i **Gruppe- eller brukernavn**, velg **Tillat** fra **Endre** og klikk deretter på **OK**.

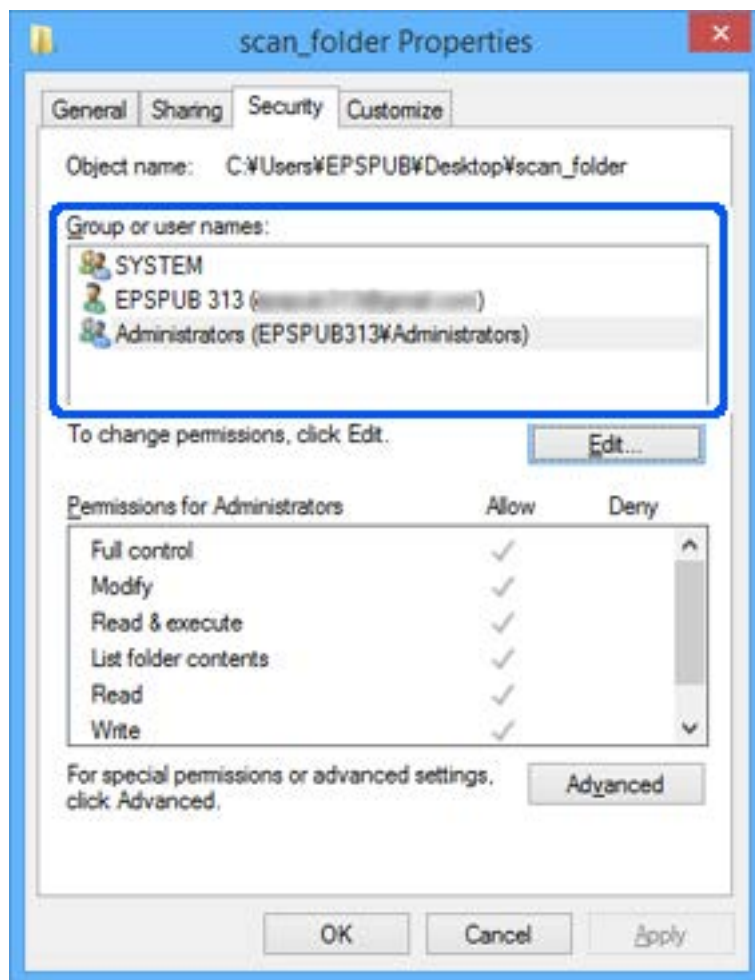


12. Klikk på **OK** for å lukke skjermen og gå tilbake til Egenskaper-vinduet.

Merknad:

Du kan sjekke hvilke grupper eller brukere som har tilgang til nettverksmappen via **Sikkerhet-fanen > Gruppe- eller brukernavn**.

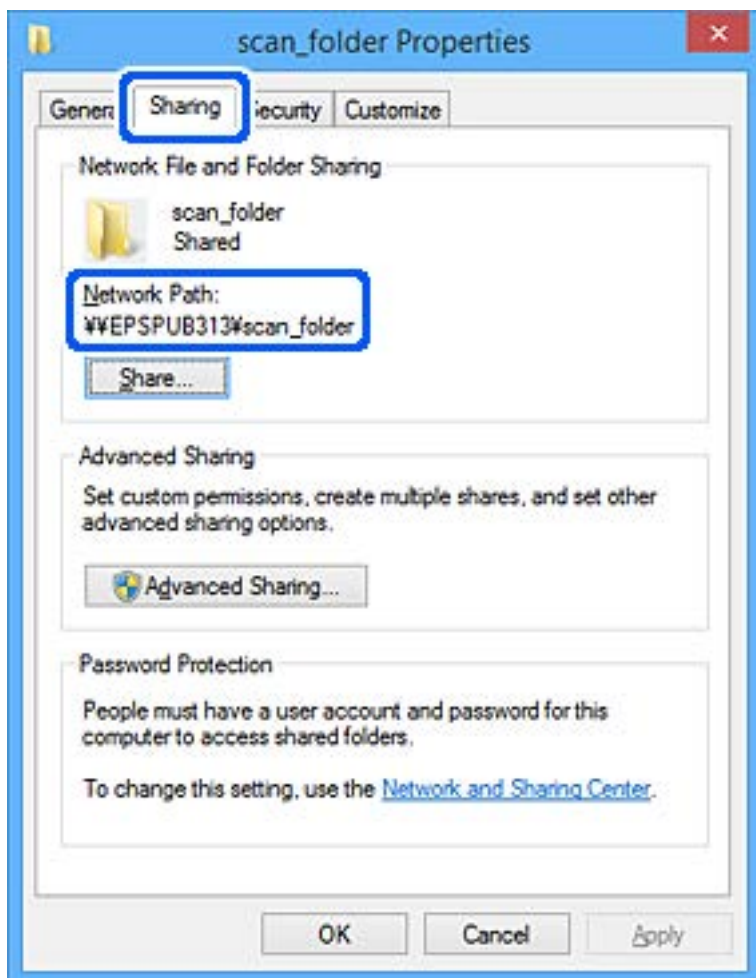
Eksempel: når brukeren som er logget på datamaskinen og administratorene kan åpne nettverksmappen



13. Velg **Deling**-fanen.

Nettverksbanen til nettverksmappen vises. Dette brukes når du registrerer kontaktene dine for skanneren. Skriv den ned.

Eksempel: \\EPSPUB313\scan_folder



14. Klikk på **Lukk** eller **OK** for å lukke vinduet.

Etter dette er du ferdig med å opprette en nettverksmappe.

Gjøre kontakter tilgjengelig

Registrering av destinasjoner i skannerens kontaktliste gjør det enkelt å skrive inn destinasjonen når du skanner. Du kan registrere følgende destinasjonstyper i kontaktlisten. Du kan registrere opptil 300 oppføringer.

Merknad:

Du kan også bruke LDAP-serveren (LDAP-søk) for å skrive inn destinasjonen.

E-post	Destinasjon for e-post. Du må konfigurere innstillingene for e-postserveren på forhånd.
Nettverksmappe	Destinasjon for skannedata. Du må forberede nettverksskannen på forhånd.

Relatert informasjon

➔ [“Samarbeid mellom LDAP-server og brukere” på side 59](#)

Sammenlikning av kontaktkonfigurasjon

Det finnes tre verktøy for å konfigurere skannerens kontakter: Web Config, Epson Device Admin og skannerens kontrollpanel. Forskjellene mellom de tre verktøyene vises i tabellen nedenfor.

Funksjoner	Web Config*	Epson Device Admin	Skannerens kontrollpanel
Registrere et mål	✓	✓	✓
Redigere et mål	✓	✓	✓
Legge til en gruppe	✓	✓	✓
Redigere en gruppe	✓	✓	✓
Slette et mål eller grupper	✓	✓	✓
Slette alle mål	✓	✓	–
Importere en fil	✓	✓	–
Eksportere til en fil	✓	✓	–

* Logg på som administrator for å angi innstillinger.

Registrere et mål for kontakter ved hjelp av Web Config

Merknad:

Du kan også registrere kontakter på skannerens kontrollpanel.

1. Gå inn på Web Config og velg **Skann**-fanen > **Kontakter**.
2. Velg et tall som du vil registrere og klikk deretter **Rediger**.
3. Skriv inn **Navn** og **Indeksord**.
4. Velg destinasjonstype som **Type**-alternativet.

Merknad:

*Du kan ikke endre **Type**-alternativet etter at registreringen er fullført. Hvis du ønsker å endre type, slett destinasjonen og registrer deg på nytt.*

5. Angi en verdi for hvert element, og klikk deretter **Bruk**.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Destinasjonens innstillingspunkter

Artikler	Innstillinger og forklaring
Vanlige innstillinger	
Navn	Skriv inn et navn til visning i kontakter, med maksimalt 30 tegn i Unicode (UTF-16). Hvis du ikke angir dette, la det stå tomt.
Indeksord	Angi et navn på 30 tegn eller mindre i Unicode (UTF-16) for å søke etter kontaktene på skannerens kontrollpanel. Hvis du ikke angir dette, la det stå tomt.
Type	Velg adressetypen som du vil registrere.
Tilordne hyppig bruk	Velg for å angi den registrerte adressen som en hyppig brukt adresse. Når du angir som en hyppig brukt adresse, vil det vises på den øverste skjermen av skanning, og du kan angi destinasjonen uten å vise kontaktene.
E-post	
E-postadresse	Skriv inn mellom 1 og 255 tegn ved hjelp av A–Z a–z 0–9 ! # \$ % & ' * + - . / = ? ^ _ { } ~ @.
Nettverksmappe (SMB)	
Lagre til	\\«Mappebane» Angi plassering for målmappen, mellom 1 og 253 tegn i Unicode (UTF-16), uten «\». Angi nettverksbanen som vises på mappens skjermbilde for egenskaper. Se følgende for mer informasjon om hvordan du angir nettverksbanen. "Opprette en nettverksmappe" på side 46
Brukernavn	Skriv inn et brukernavn på maksimalt 30 tegn (UTF-16) for å få tilgang til en nettverksmappe. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F).
Passord	Skriv inn et passord på mellom 0 og 20 tegn i Unicode (UTF-16) for å få tilgang til en nettverksmappe. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F).
FTP	
Sikker forbindelse	Velg FTP eller FTPS avhengig av filoverføringsprotokollen FTP-serveren støtter. Velg FTPS for å la skanneren kommunisere med sikkerhetstiltak.
Lagre til	Skriv inn servernavnet mellom 1 og 253 tegn i Unicode (UTF-16), uten «ftp://» eller «ftps://».
Brukernavn	Skriv inn et brukernavn på maksimalt 30 tegn (UTF-16) for å få tilgang til en FTP-server. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F). Hvis serveren tillater anonyme tilkoblinger, skriver du inn et brukernavn som Anonymous og FTP. Hvis du ikke angir dette, la det stå tomt.
Passord	Skriv inn et passord på mellom 0 og 20 tegn i Unicode (UTF-16) for å få tilgang til en FTP-server. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F). Hvis du ikke angir dette, la det stå tomt.
Tilkoblingsmodus	Velg tilkoblingsmodus fra menyen. Hvis det er angitt en brannmur mellom skanneren og FTP-serveren, velger du Passivt modus .
Portnummer	Skriv inn FTP-serverens portnummer mellom 1 og 65 535.

Artikler	Innstillinger og forklaring
Sertifikatvalidering	Sertifikatet for FTP-serveren valideres når dette er aktivert. Dette er tilgjengelig når FTPS er valgt for Sikker forbindelse . For å konfigurere må du importere CA-sertifikat til skanneren.
SharePoint(WebDAV)*	
Sikker forbindelse	Velg HTTP eller HTTPS avhengig av filoverføringsprotokollen serveren støtter. Velg HTTPS for å la skanneren kommunisere med sikkerhetstiltak.
Lagre til	Skriv inn servernavnet mellom 1 og 253 tegn i Unicode (UTF-16), uten «http://» eller «https://».
Brukernavn	Skriv inn et brukernavn på maksimalt 30 tegn (UTF-16) for å få tilgang til en server. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F). Hvis du ikke angir dette, la det stå tomt.
Passord	Skriv inn et passord på mellom 0 og 20 tegn i Unicode (UTF-16) for å få tilgang til en server. Unngå å bruke kontrolltegn (0x00 til 0x1F, 0x7F). Hvis du ikke angir dette, la det stå tomt.
Sertifikatvalidering	Sertifikatet for serveren valideres når dette er aktivert. Dette er tilgjengelig når HTTPS er valgt for Sikker forbindelse . For å konfigurere må du importere CA-sertifikat til skanneren.
Proxy-server	Velg om du skal bruke en proxy-server.

* SharePoint Online støttes ikke ved skanning til en nettverksmappe fra skannerens kontrollpanel.

Hvis du vil lagre det skannede elementet til SharePoint Online, bruker du Document Capture Pro etter at du har installert SharePoint Online Connector. Se Document Capture Pro-håndboken for mer informasjon.

<https://support.epson.net/dcp/>

Registrere mål som en gruppe med Web Config

Hvis destinasjonstypen er satt til **E-post**, kan du registrere destinasjonen som en gruppe.

1. Gå inn på Web Config og velg **Skann**-fanen > **Kontakter**.
2. Velg et tall som du vil registrere og klikk deretter **Rediger**.
3. Velg en gruppe fra **Type**.
4. Klikk **Velg for Kontakt(er) for Gruppe**.
De tilgjengelige destinasjonene vises.
5. Velg den destinasjonen du vil registrere i gruppen, og klikk deretter **Velg**.
6. Skriv inn et **Navn** og **Indeksord**.
7. Velg om du tilordne den registrerte gruppen til ofte brukte gruppen.

Merknad:

Destinasjoner kan registreres til flere grupper.

8. Klikk på **Bruk**.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Sikkerhetskopiere og importere kontakter

Ved hjelp av Web Config eller andre vektøy kan du sikkerhetskopiere og importere kontakter.

For Web Config kan du sikkerhetskopiere kontakter ved å eksportere skanneinnstillingene som inkluderer kontakter. Den eksporterte filen kan redigeres fordi den eksporteres som en binær fil.

Kontaktene overskrives når skanneinnstillingene importeres til skanneren.

For Epson Device Admin kan kun kontakter eksporteres fra enhetens skjerm bilde for egenskaper. Hvis du ikke eksporterer sikkerhetsrelaterte elementer, kan du også redigere de eksporterte kontaktene og importere dem, ettersom dette kan lagres som en SYLK- eller CSV-fil.

Importere kontakter med Web Config

Hvis du har en skanner som gir deg mulighet til å sikkerhetskopiere kontakter og som er kompatibel med denne skanneren, kan du enkelt registrere kontakter ved å importere sikkerhetskopifilen.

Merknad:

Hvis du vil ha instruksjoner for hvordan du sikkerhetskopierer skannerens kontakter, kan du se bruksanvisninger som følger med skanneren.

Følg trinnene under for å importere kontakter til denne skanneren.

1. Åpne Web Config og velg **Enhetsadministrasjon**-fanen > **Innstillingsverdi for eksportering og importering** > **Importer**.
2. Velg sikkerhetskopifilen du opprettet i **Fil**, angi passordet og klikk på **Neste**.
3. Velg avmerkingsboksen **Kontakter** og klikk på **Neste**.

Sikkerhetskopiere kontakter med Web Config

Data for kontakter kan gå tapt på grunn av feilfunksjon i skanneren. Vi anbefaler at du tar en sikkerhetskopi av dataen når du oppdaterer den. Epson skal ikke holdes ansvarlig for eventuelle tap av data, for sikkerhetskopiering eller gjenoppretting av data og/eller innstillinger, selv i løpet av en garantiperiode.

Med Web Config, kan du sikkerhetskopiere kontaktdata som er lagret på skanneren til datamaskinen.

1. Gå inn på Web Config, og velg deretter **Enhetsadministrasjon**-fanen > **Innstillingsverdi for eksportering og importering** > **Eksporter**.
2. Velg avmerkingsboksen **Kontakter** under kategorien **Skann**.
3. Skriv inn et passord for å kryptere den eksporterte filen.
Du trenger passordet for å importere filen. La dette stå tomt hvis du ikke ønsker å kryptere filen.
4. Klikk på **Eksporter**.

Eksportering og grupperegistrering av kontakter med verktøyet

Hvis du bruker Epson Device Admin, kan du velge å kun sikkerhetskopiere kontaktene og redigere de eksporterte filene, og deretter registrere alle samtidig.

Dette er nyttig hvis du ønsker å kun sikkerhetskopiere kontaktene, eller når du bytter ut skanneren og ønsker å overføre kontaktene fra den gamle skanneren til den nye.

Eksportere kontakter

Lagre kontaktinformasjonen til filen.

Du kan redigere filer lagret i SYLK- eller csv-format ved bruk av en regnearksapplikasjon eller et tekstbehandlingsprogram. Du kan registrere alle på en gang etter at informasjonen er slettet eller lagt til.

Informasjonen som inkluderer sikkerhetslementer som passord og personlig informasjon, kan lagres i binærformat med passord. Du kan ikke endre filen. Dette kan brukes som sikkerhetskopifil av informasjonen, inkludert sikkerhetslementene.

1. Start Epson Device Admin.
2. Velg **Devices** på sidestolpen med oppgavemeny.
3. Velg enheten du vil konfigurere fra enhetslisten.
4. Klikk **Device Configuration** på **Home**-fanen på båndmenyen.

Når et passord har blitt angitt for administratoren, skriver du inn passordet og klikker **OK**.

5. Klikk **Common > Contacts**.
6. Velg eksportformat fra **Export > Export items**.

All Items

Eksporter den krypterte binærfilen. Velg når du ønsker å inkludere sikkerhetslementer som passord og personlig informasjon. Du kan ikke endre filen. Hvis du velger den, må du angi passordet. Klikk **Configuration** og angi et passord mellom 8 og 63 tegn i ASCII. Dette passordet kreves når binærfilen importeres.

Items except Security Information

Eksporter filene i SYLK- eller csv-format. Velg når du ønsker å redigere informasjonen til den eksporterte filen.

7. Klikk på **Export**.
8. Spesifiser stedet hvor filen skal lagres, velg filtype og klikk **Save**.
Fullføringsmeldingen vises.
9. Klikk på **OK**.
Kontroller at filen er lagret til det spesifiserte stedet.

Importere kontakter

Importer kontaktinformasjonen fra filen.

Du kan importere filene lagret i SYLK- eller CSV-format, eller den sikkerhetskopierte binærfilen som er inkludert i sikkerhetselementene.

1. Start Epson Device Admin.
2. Velg **Devices** på sidestolpen med oppgavemeny.
3. Velg enheten du vil konfigurere fra enhetslisten.
4. Klikk **Device Configuration** på **Home**-fanen på båndmenyen.
Når et passord har blitt angitt for administratoren, skriver du inn passordet og klikker **OK**.
5. Klikk **Common > Contacts**.
6. Klikk **Browse** på **Import**.
7. Velg filen du vil importere og klikk deretter **Open**.
Når du velger binærfilen, skal du skrive inn passordet du skrev inn da du eksporterte filen **Password**.
8. Klikk på **Import**.
Bekreftelsesskjerm bildet vises.
9. Klikk på **OK**.
Valideringsresultatet vises.
 - Edit the information read
Klikk når du ønsker å endre informasjonen individuelt.
 - Read more file
Klikk når du ønsker å importere flere filer.
10. Klikk **Import**, og klikk deretter **OK** på skjerm bildet for fullføring av importering.
Gå tilbake til skjerm bildet for enhetens egenskaper.
11. Klikk på **Transmit**.
12. Klikk **OK** på bekreftelsesmeldingen.
Innstillingene sendes til skanneren.
13. Klikk **OK** på skjerm bildet for fullført sending.
Skannerinformasjonen er oppdatert.
Åpne kontaktene fra Web Config eller skannerens kontrollpanel, og kontroller deretter at kontakten er oppdatert.

Samarbeid mellom LDAP-server og brukere

Ved samarbeid med LDAP-serveren, kan du bruke adresseinformasjonen registrert på LDAP-serveren som destinasjon for e-post.

Konfigurere LDAP-serveren

For å bruke informasjonen til LDAP-serveren, må den registreres på skanneren.

1. Gå inn på Web Config og velg **Nettverk**-fanen > **LDAP-server** > **Grunnleggende**.
2. Angi en verdi for hvert element.
3. Velg **OK**.
Innstillingene du har valgt, vises.

Innstillingselementer for LDAP-server

Artikler	Innstillinger og forklaring
Bruk LDAP-server	Velg Bruk eller Ikke bruk .
LDAP-serveradresse	Skriv inn adressen til LDAP-serveren. Skriv inn mellom 1 og 255 tegn i enten IPv4-, IPv6- eller FQDN-format. Med FQDN-formatet kan du bruke alfanumeriske tegn i ASCII (0x20–0x7E) og «-», bortsett fra i starten og slutten av adressen.
LDAP-serverportnummer	Skriv inn LDAP-serverens portnummer mellom 1 og 65 535.
Sikker forbindelse	Angi godkjenningmetoden når skanneren får tilgang til LDAP-serveren.
Sertifikatvalidering	Når dette er aktivert, er LDAP-serverens sertifikat validert. Vi anbefaler at dette settes til Aktiver . For å konfigurere må CA-sertifikat være importert til skanneren.
Tidsavbrudd for søk (sek)	Angi tiden for å søke før tidsavbrudd mellom 5 og 300.
Godkjenningmetode	Velg en av metodene. Hvis du velger Kerberos-autentisering , velger du Kerberos-innstillinger for å angi innstillinger for Kerberos. For å gjennomføre Kerberos-autentisering, kreves følgende omgivelser. <input type="checkbox"/> Skanneren og DNS-serveren kan kommunisere. <input type="checkbox"/> Klokkeslettet til skanneren, KDC-serveren og serveren som kreves for godkjenning (LDAP-server, SMTP-server, filserver) er synkroniserte. <input type="checkbox"/> Når tjenesteserveren er tilordnet som IP-adressen, er tjenesteserverens FQDN registrert på DNS-serverens reverserte oppslagssone.
Kerberos-område som skal brukes	Hvis du velger Kerberos-autentisering for Godkjenningmetode , velger du Kerberos-riket som du vil bruke.
Administrator-DN / Brukernavn	Skriv inn brukernavnet for LDAP-serveren på 128 tegn eller mindre i Unicode (UTF-8). Du kan ikke bruke kontrolltegn, som 0x00–0x1F og 0x7F. Denne innstillingen brukes ikke når Anonym autentisering er valgt som Godkjenningmetode . Hvis du ikke angir dette, la det stå tomt.
Passord	Skriv inn passordet for LDAP-servergodkjenning på 128 tegn eller mindre i Unicode (UTF-8). Du kan ikke bruke kontrolltegn, som 0x00–0x1F og 0x7F. Denne innstillingen brukes ikke når Anonym autentisering er valgt som Godkjenningmetode . Hvis du ikke angir dette, la det stå tomt.

Kerberos-innstillinger

Hvis du velger **Kerberos-autentisering** som **Godkjenningstype** for **LDAP-server** > **Grunnleggende**, foretar du følgende Kerberos-innstillinger fra **Nettverk**-fanen > **Kerberos-innstillinger**. Du kan registrere opptil 10 innstillinger for Kerberos-innstillingene.

Artikler	Innstillinger og forklaring
Område (domene)	Skriv inn området for Kerberos-godkjenning med maksimalt 255 i ASCII (0x20–0x7E). Hvis du ikke registrerer dette, la det stå tomt.
KDC-adresse	Skriv inn adressen til Kerberos-autentiseringsserveren. Skriv inn 255 tegn eller mindre i enten IPv4, IPv6 eller FQDN-format. Hvis du ikke registrerer dette, la det stå tomt.
Portnummer (Kerberos)	Skriv inn Kerberos-serverens portnummer mellom 1 og 65535.

Konfigurere søkeinnstillinger for LDAP-serveren

Når du konfigurerer søkeinnstillingene, kan du bruke e-postadressen registrert på LDAP-serveren.

- Gå inn på Web Config og velg **Nettverk**-fanen > **LDAP-server** > **Søkeinnstillinger**.
- Angi en verdi for hvert element.
- Klikk **OK** for å vise innstillingsresultatet.
Innstillingene du har valgt, vises.

Innstillingselementer for søk på LDAP-server

Artikler	Innstillinger og forklaring
Søkebase (unikt navn)	Hvis du vil søke på et tilfeldig domene, angir du domenenavnet til LDAP-serveren. Skriv inn mellom 0 og 128 tegn i Unicode (UTF-8). Hvis du ikke søker etter en vilkårlig attributt, la dette stå tomt. Eksempel på lokal serverkatalog: dc=server,dc=local
Antall søkeoppføringer	Angi antall søkeoppføringer mellom 5 og 500. Det angitte antallet av søkte oppføringer lagres og vises midlertidig. Selv om antall søkeoppføringer er over det angitte antallet og det vises en feilmelding, kan søket bli fullført.
Brukernavnegenskap	Angi attributtnavn som skal vises når du søker etter brukernavn. Skriv inn mellom 1 og 255 tegn i Unicode (UTF-8). Det første tegnet må være a–z eller A–Z. Eksempel: cn, uid
Brukernavnvisningsegenskap	Angi attributtnavn som skal vises som brukernavnet. Skriv inn mellom 0 og 255 tegn i Unicode (UTF-8). Det første tegnet må være a–z eller A–Z. Eksempel: cn, sn
E-postadresseegenskap	Angi attributtnavn som skal vises når du søker etter e-postadresser. Skriv inn en kombinasjon av 1 og 255 tegn ved hjelp av A–Z, a–z, 0–9 og -. Det første tegnet må være a–z eller A–Z. Eksempel: post

Artikler	Innstillinger og forklaring
Vilkårlig egenskap 1 - Vilkårlig egenskap 4	Du kan angi andre vilkårlige attributter for å søke etter. Skriv inn mellom 0 og 255 tegn i Unicode (UTF-8). Det første tegnet bør være a-z eller A-Z. La dette feltet stå tomt hvis du ikke vil søke etter tilfeldige attributter. Eksempel: o, ou

Kontrollere LDAP-servertilkoblingen

Utfører tilkoblingstesten til LDAP-serveren ved hjelp av parameteren angitt i **LDAP-server > Søkeinnstillinger**.

- Gå inn på Web Config og velg **Nettverk**-fanen > **LDAP-server** > **Tilkoblingstest**.
- Velg **Start**.
Tilkoblingstest startet. Etter testen vil kontrollrapporten vises.

Testreferanser for LDAP-servertilkobling

Meldinger	Forklaring
Tilkoblingstesten var vellykket.	Denne meldingen vises når tilkoblingen til serveren er vellykket.
Tilkoblingstesten mislyktes. Kontroller innstillingene.	Denne meldingen vises av følgende årsaker: <input type="checkbox"/> Det er feil adresse eller portnummer til LDAP-serveren. <input type="checkbox"/> Det oppstod et tidsavbrudd. <input type="checkbox"/> Ikke bruk er valgt som Bruk LDAP-server . <input type="checkbox"/> Hvis Kerberos-autentisering er valgt som Godkjenning metode , innstillinger som Område (domene) , KDC-adresse og Portnummer (Kerberos) er feil.
Tilkoblingstesten mislyktes. Kontroller dato og klokkeslett på produktet eller serveren.	Denne meldingen vises når tilkoblingen mislykkes fordi tidsinnstillingene for skanneren og LDAP-serveren ikke samsvarer.
Autentisering mislyktes. Kontroller innstillingene.	Denne meldingen vises av følgende årsaker: <input type="checkbox"/> Brukernavn og/eller Passord er feil. <input type="checkbox"/> Hvis Kerberos-autentisering er valgt som Godkjenning metode kan ikke klokkeslett/dato konfigureres.
Får ikke tilgang til produktet før behandlingen er fullført.	Denne meldingen vises når skanneren er opptatt.

Konfigurere AirPrint

Åpne Web Config, velg fanen **Nettverk** og velg deretter **AirPrint-innstilling**.

Artikler	Forklaring
Bonjour servicenavn	Angi navnet på en Bonjour-tjeneste med ASCII-tekst (0x20–0x7E) og opptil 41 tegn.
Bonjour-plassering	Angi en beskrivelse av plasseringen til skanneren med Unicode-tekst (UTF-8) og inntil 127 byte.
Wide-Area Bonjour	Angi hvorvidt Wide-Area Bonjour skal brukes. Hvis du bruker det, må skanneren være registrert på DNS-serveren for å kunne søke etter skanneren over segmentet.
Aktiver AirPrint	Aktiverer Bonjour og AirPrint (Skannetjeneste). Denne knappen er bare tilgjengelig når AirPrint er deaktivert. Merknad: <i>Hvis AirPrint er deaktivert, er Mopria-skanning fra Chromebook og Windows og Mopria Scan-appen også deaktivert.</i>

Problemer ved forberedelse av nettverksskanning

Hint for å løse problemer

Kontrollere feilmeldingene

Når det har oppstått et problem, må du først kontrollere om det står noen meldinger på skannerens kontrollpanel eller driverskjerm. Hvis du har angitt varsling på e-post når hendelsene oppstår, kan du raskt finne statusen.

Kontrollere kommunikasjonsstatusen

Kontroller kommunikasjonsstatusen til server- eller klientdatamaskinen ved hjelp av kommandoer som ping og ipconfig.

Tilkoblingstest

Utfør tilkoblingstesten fra skanneren for å kontrollere tilkoblingen mellom skanneren og e-postservieren. Kontroller også tilkoblingen fra klientdatamaskinen til serveren for å kontrollere kommunikasjonsstatusen.

Initialisere innstillingene

Hvis innstillingene og kommunikasjonsstatusen ikke viser noe problem, kan problemet kanskje løses ved å deaktivere eller initialisere skannerens nettverksinnstillinger, og deretter konfigurere disse på nytt.

Får ikke tilgang til Web Config

IP-adressen er ikke tilordnet til skanneren.

Løsninger

En gyldig IP-adresse kan ikke tilordnes til skanneren. Konfigurer IP-adressen ved hjelp av skannerens kontrollpanel. Du kan bekrefte gjeldende innstillingsinformasjon fra skannerens kontrollpanel.

Nettleseren støtter ikke krypteringsstyrken for SSL/TLS.

Løsninger

SSL/TLS har Krypteringsstyrke. Du kan åpne Web Config ved hjelp av en nettleser som støtter bulkkryptering, som angitt under. Kontroller at du bruker en støttet nettleser.

- 80 bit: AES256/AES128/3DES
- 112 bit: AES256/AES128/3DES
- 128 bit: AES256/AES128
- 192 bit: AES256
- 256 bit: AES256

CA-signert sertifikat er utløpt.

Løsninger

Hvis det er et problem med sertifikatets utløpsdato, vises «Sertifikatet er utløpt» ved tilkobling til Web Config med SSL/TLS-kommunikasjon (https). Hvis meldingen vises før utløpsdatoen, kontrollerer du at skannerens dato er riktig konfigurert.

Sertifikatets og skannerens fellesnavn samsvarer ikke.

Løsninger

Hvis sertifikatets og skannerens fellesnavn ikke samsvarer, vises meldingen «Navnet på sikkerhetssertifikatet samsvarer ikke...» når Web Config åpnes ved hjelp av SSL/TLS-kommunikasjon (https). Dette skjer fordi følgende IP-adresser ikke samsvarer.

- Skannerens IP-adresse som er angitt for fellesnavn for å opprette et Selvsignert sertifikat eller CSR
- IP-adressen som er angitt til nettleseren når Web Config kjøres

Oppdater sertifikatet for Selvsignert sertifikat.

Ta sertifikatet igjen for skanneren for CA-signert sertifikat.

Innstillingen av lokal adresse for proxy-serveren er ikke angitt til nettleseren.

Løsninger

Når skanneren er innstilt til å bruke en proxyserver, må nettleseren konfigureres til å ikke koble til den lokale adressen via proxyserveren.

- Windows:

Velg **Kontrollpanel > Nettverk og Internett > Alternativer for Internett > Tilkoblinger > LAN-innstillinger > Proxy-server**, og deretter konfigurerer du at proxy-serveren ikke skal brukes for LAN (lokale adresser).

- Mac OS:

Velg **Systemvalg** (eller **Systeminnstillinger**) > **Nettverk** > **Avansert** > **Proxyer**, og registrer deretter den lokale adressen for **Ignorer proxyinnstillinger for disse vertene og domenene**.

Eksempel:

192.168.1.*: Lokal adresse 192.168.1.XXX, nettverksmaske 255.255.255.0

192.168.*.*: Lokal adresse 192.168.XXX.XXX, nettverksmaske 255.255.0.0

DHCP er deaktivert i datamaskinens innstillinger.

Løsninger

Hvis DHCP for å hente en IP-adresse deaktiveres automatisk på datamaskinen, får du ikke tilgang til Web Config. Aktiver DHCP.

Eksempel for Windows 10:

Åpne kontrollpanelet og klikk **Nettverk og Internett** > **Nettverks- og delingssenter** > **Endre adapterinnstillinger**. Åpne Egenskaper-skjermbildet for tilkoblingen du bruker, og åpne deretter egenskaper-skjermbildet for **Internettprotokoll versjon 4 (TCP/IPv4)** eller **Internettprotokoll versjon 6 (TCP/IPv6)**. Kontroller at **Hent en IP-adresse automatisk** er valgt på skjermbildet som vises.


Tilpasse kontrollpanelskjermen

Registrere Forhåndsinn.	67
Redigere startskjermen til kontrollpanelet.	69

Registrere Forhåndsinn

Du kan registrere ofte brukte skanneinnstillinger som **Forhåndsinn**. Du kan registrere opp til 48 forhåndsinnstillinger.

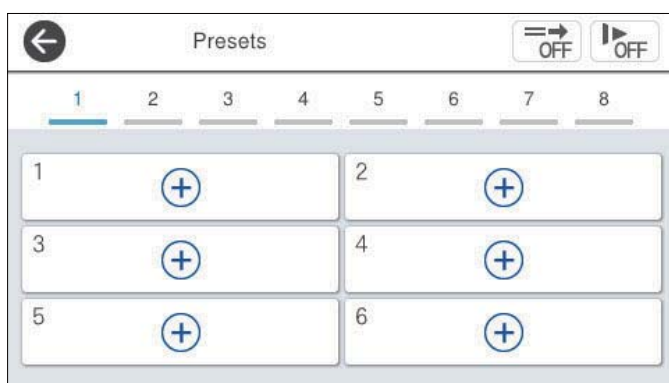
Merknad:

- Du kan registrere nåværende innstillinger ved å velge  på skjermbildet for start av skanning.
- Du kan også registrere **Forhåndsinnstillinger** i Web Config.
Velg **Skann-fanen > Forhåndsinnstillinger**.
- Hvis du velger **Skann til datamaskin** når du registrerer deg, kan du registrere jobben du opprettet i Document Capture Pro som **Forhåndsinnstillinger**. Dette er kun tilgjengelig for datamaskiner som er koblet sammen over et nettverk. Registrer jobben i Document Capture Pro på forhånd.
- Hvis autentifikasjonsfunksjonen er aktivert, kan kun administratoren registrere **Forhåndsinnstillinger**.

1. Velg **Forhåndsinn** på startskjermen til skannerens kontrollpanel.




2. Velg .



3. Velg menyen du vil bruke for å registrere en forhåndsinnstilling.

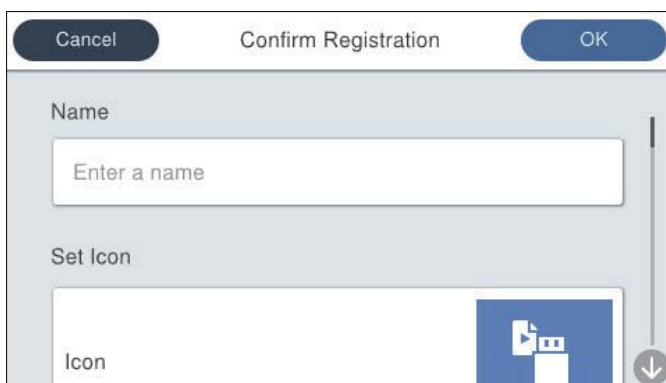


4. Angi hvert element og velg deretter .

Merknad:


Når du velger **Skann til datamaskin**, velger du datamaskinen hvor Document Capture Pro er installert. Deretter velger du en registrert jobb. Dette er kun tilgjengelig for datamaskiner som er koblet sammen over et nettverk.

5. Utfør forhåndsinnstillingene.
 - Navn:** Angi navnet.
 - Angi Ikon:** Angi bildet og fargen til bildet som skal vises.
 - Hurtigsende-innstilling:** Begynner å skanne umiddelbart uten bekreftelse når forhåndsinnstillingen velges.
 - Innhold:** Kontrollerer skanneinnstillingene.



6. Velg OK.

Menyalternativer for Forhåndsinnss

Du kan endre forhåndsinnstillinger ved å velge  i hver forhåndsinnstilling.

Endre navn:

Endrer navnet til forhåndsinnstillingen.

Endre Ikon:

Endrer ikonbildet og fargen til forhåndsinnstillingen.

Hurtigsende-innstilling:

Begynner å skanne umiddelbart uten bekreftelse når forhåndsinnstillingen velges.

Endre posisjon:

Endre visningsrekkefølgen til forhåndsinnstillingene.

Slett:

Sletter forhåndsinnstillingen.

Legg til eller fjern Ikon på Hjem:

Legger til eller fjerner ikonet til forhåndsinnstillingen fra startskjermen.

Bekreft detaljer:

Se innstillingene til en forhåndsinnstilling. Du kan laste inn forhåndsvisningen ved å velge **Bruk denne innstillingen**.

Redigere startskjermen til kontrollpanelet

Du kan tilpasse startskjermen ved å velge **Innst.** > **Rediger Startskjerm** på skannerens kontrollpanel.

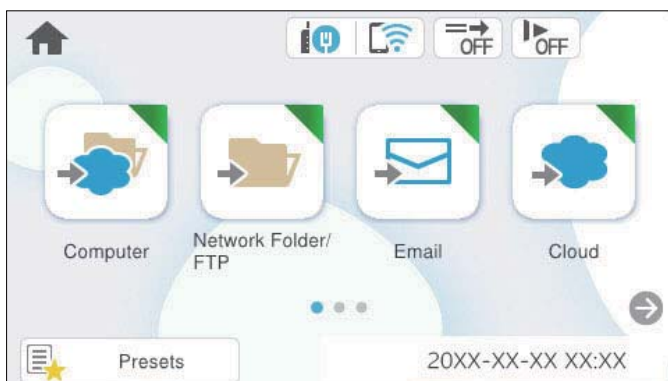
- Layout: Endrer visningsmetoden til menyikonene.
[“Endre Layout på startskjermen” på side 69](#)
- Legg til ikon: Legger til ikoner i **Forhåndsinn**-innstillingene du har angitt, eller gjenoppretter ikoner som har blitt fjernet fra skjermen.
[“Legg til ikon” på side 70](#)
- Fjern ikon: Fjerner ikoner fra startskjermen.
[“Fjern ikon” på side 71](#)
- Flytt ikon: Endrer visningsrekkefølgen til ikonene.
[“Flytt ikon” på side 72](#)
- Gjenopprett standard ikonvisning: Gjenoppretter standard skjerminnstillinger for startskjermen.

Endre Layout på startskjermen

1. Velg **Innst.** > **Rediger Startskjerm** > **Layout** på skannerens kontrollpanel.


2. Velg **Linje** eller **Matrise**.

Linje:



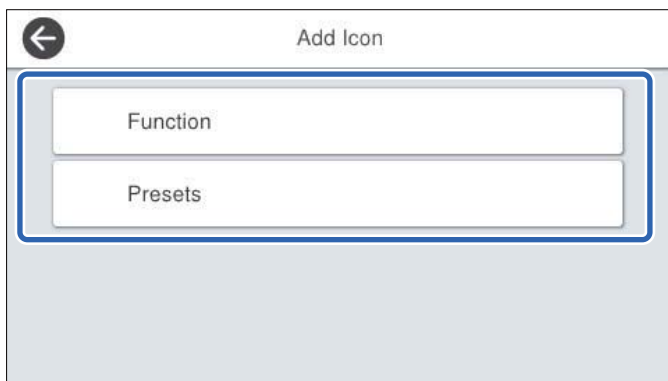
Matrise:



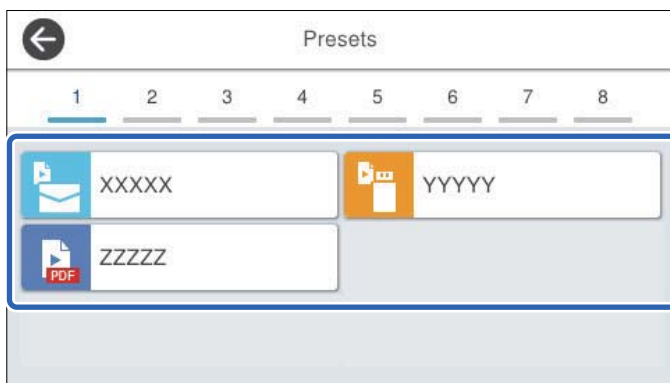
3. Velg  for å gå tilbake og kontrollere startskjermen.

Legg til ikon

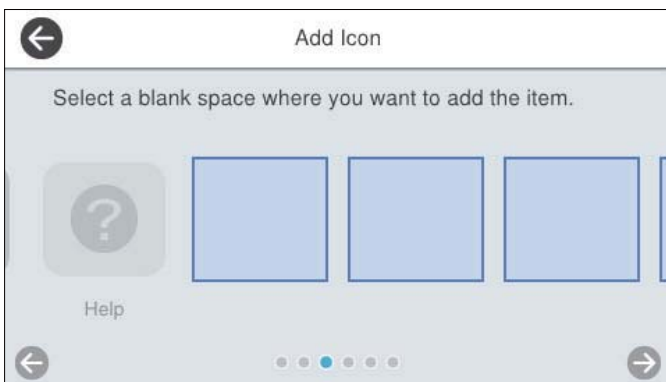
1. Velg **Innst.** > **Rediger Startskjerm** > **Legg til ikon** på skannerens kontrollpanel.
2. Velg **Funksjon** eller **Forhåndsinn**.
 - Funksjon: Viser standardfunksjonene som vises for startskjermen.
 - Forhåndsinn: Viser registrerte forhåndsinnstillinger.




3. Velg elementet du vil legge til startskjermen.



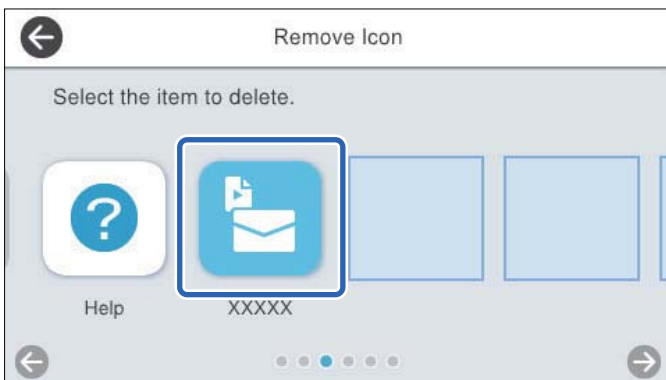
4. Velg tomrommet hvor du vil legge til elementet.
Hvis du vil legge til flere ikoner gjentar du trinn 3 til 4.




5. Velg  for å gå tilbake og kontrollere startskjermen.

Fjern ikon

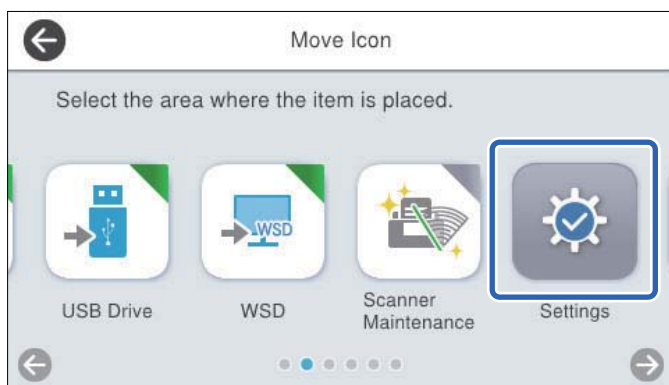
1. Velg **Innst.** > **Rediger Startskjerm** > **Fjern ikon** på skannerens kontrollpanel.
2. Velg ikonet du vil fjerne.



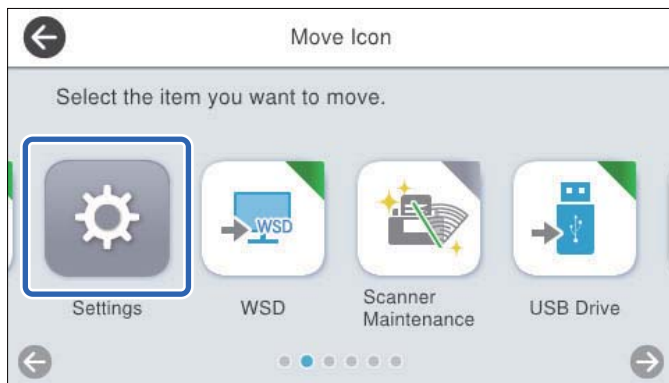
3. Velg **Ja** for å avslutte.
Hvis du vil fjerne flere ikoner gjentar du prosedyre 2 til 3.
4. Velg  for å gå tilbake og kontrollere startskjermen.


Flytt ikon

1. Velg **Innst.** > **Rediger Startskjerm** > **Flytt ikon** på skannerens kontrollpanel.
2. Velg ikonet du vil flytte.



3. Velg destinasjonsrammen.
Hvis et annet ikon allerede befinner seg i destinasjonsrammen vil det nye ikonet erstatte det gamle.



4. Velg  for å gå tilbake og kontrollere startskjermen.

Grunnleggende sikkerhetsinnstillinger

Introduksjon til produktets sikkerhetsfunksjoner.	74
Administratorinnstillinger.	74
Begrense tilgjengelige funksjoner (Tilgangskontroll).	80
Deaktivere eksternt grensesnitt.	82
Aktivere programverifisering ved oppstart.	82
Deaktivere nettverksskanning fra datamaskinen.	83
Aktivere eller deaktivere WSD-skanning.	83
Administrere en ekstern skanner.	84
Gjenopprette standardinnstillingene.	85
Informasjon om Epson Remote Services.	86
Problemløsning.	86

Introduksjon til produktets sikkerhetsfunksjoner

Dette avsnittet introduserer sikkerhetsfunksjonen til Epson-enhetene.

Funksjonsnavn	Funksjonstype	Hva skal stilles inn	Hva skal forebygges
Konfigurere administratorpassordet	Låser systeminnstillinger slik som tilkoblingskonfigurasjon for nettverk eller USB.	En administrator angir et passord for enheten. Du kan angi eller endre fra både Web Config og skannerens kontrollpanel.	Unngå ulovlig lesing og endring av informasjon som er lagret på enheten, slik som ID, passord, nettverksinnstillinger og så videre. Reduser også et bredt spekter av sikkerhetsrisikoer som lekkasje av informasjon til nettverksmiljøet eller sikkerhetspolitikk.
Innstillinger for tilgangskontroll	Hvis du logger på enheten med en brukerkonto som er forhåndsregistrert, kan du bruke enheten.	Registrer enhver brukerkonto. Du kan registrere opptil 10 brukerkontoer.	Begrensning av brukere forebygger uautorisert bruk av enheten.
Konfigurasjon for eksterne grensesnitt	Kontrollerer grensesnittet som kobler seg til enheten.	Aktiver eller deaktiver USB-tilkobling med datamaskinen.	USB-tilkobling til datamaskin: forhindrer uautorisert bruk av enheten ved å forby skanning uten å gå via nettverket.

Relatert informasjon

- ➔ [“Konfigurere administratorpassordet” på side 74](#)
- ➔ [“Deaktivere eksternt grensesnitt” på side 82](#)

Administratorinnstillinger

Konfigurere administratorpassordet

Når du angir et administratorpassord, kan du forhindre at brukeren endrer innstillinger for systembehandling. Standardverdiene er allerede angitt på kjøpstidspunktet. Du kan endre dem ved behov.

Merknad:

Følgende gir standardverdier for administratorinformasjon.

- Brukernavn (brukes bare for Web Config): ingen (tom)
- Passord: avhenger av etiketten på produktet.

Hvis det er en PASSWORD-etikett på baksiden, angir du det 8-sifrede nummeret på etiketten. Hvis det ikke er en PASSWORD-etikett der, angir du serienummeret på etiketten på baksiden av produktet som administratorpassord den første gangen.

Du kan endre administratorpassord ved å bruke enten Web Config, skannerens kontrollpanel eller Epson Device Admin. Når du bruker Epson Device Admin, bør du bruke Epson Device Admin-veiledingen.

Endre administratorpassordet med Web Config

Endre administratorpassordet i Web Config.

1. Gå inn på Web Config og velg **Produktsikkerhet**-fanen > **Endre administratorpassord**.
2. Angi den nødvendige informasjonen i **Nåværende passord**, **Brukernavn**, **Nytt passord** og **Bekreft nytt passord**.

Det nye passordet må være mellom 8 og 20 tegn langt og inneholde kun alfanumeriske tegn og symboler med én byte.

Merknad:

Følgende gir standardverdier for administratorinformasjon.

Brukernavn: ingen (tomt)

Passord: avhenger av etiketten på produktet.

Hvis det er en PASSWORD-etikett på baksiden, angir du det 8-sifrede nummeret på etiketten. Hvis det ikke er en PASSWORD-etikett der, angir du serienummeret på etiketten på baksiden av produktet som administratorpassord den første gangen.



Forsiktighetsregel:

Forsikre deg om at du husker administratorpassordet du angir. Passordet kan ikke tilbakestilles om du glemmer det. Hvis du glemmer det, må du be om hjelp fra servicepersonell.

3. Velg **OK**.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Endre administratorpassord fra skannerens kontrollpanel

Du kan endre administratorpassord fra skannerens kontrollpanel.

1. Velg **Innst.** på skannerens kontrollpanel.
2. Velg **Systemadministrasjon** > **Administratorinnstillinger**.
3. Velg **Adminpassord** > **Endre**.
4. Angi det nåværende passordet.

Merknad:

Det opprinnelige administratorpassordet (standard) på kjøpstidspunktet varierer avhengig av etiketten på produktet. Hvis det er en PASSWORD-etikett på baksiden, angir du det 8-sifrede nummeret på etiketten. Hvis det ikke er en PASSWORD-etikett der, angir du serienummeret på etiketten på baksiden av produktet som administratorpassord den første gangen.

5. Angi det nye passordet.

Det nye passordet må være mellom 8 og 20 tegn langt og inneholde kun alfanumeriske tegn og symboler med én byte.



Forsiktighetsregel:

Forsikre deg om at du husker administratorpassordet du angir. Passordet kan ikke tilbakestilles om du glemmer det. Hvis du glemmer det, må du be om hjelp fra servicepersonell.


6. Angi det nye passordet igjen for å bekrefte.

Det vises en fullføringsmelding.

Bruke Låsinnstilling for kontrollpanelet

Du kan bruke Låsinnstilling til å låse kontrollpanelet og hindre at brukere endrer elementer tilknyttet systeminnstillingene.

Konfigurere Låsinnstilling fra kontrollpanelet

1. Hvis du vil avbryte **Låsinnstilling** når det er aktivert, kan du trykke på  øverst til høyre på Hjem-skjermen for å logge inn som administrator.



vises ikke når **Låsinnstilling** er deaktivert. Hvis du vil aktivere denne innstillingen, går du videre til neste trinn.

2. Velg **Innst.**.
3. Velg **Systemadministrasjon > Administratorinnstillinger**.
4. Velg **På** eller **Av** som **Låsinnstilling**.

Angi Låsinnstilling fra Web Config

1. Velg **Enhetsadministrasjon**-fanen > **Kontrollpanel**.
2. Velg **På** eller **Av** for **Panellås**.
3. Klikk på **OK**.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Låsinnstilling-elementer i Innst.-menyen

Dette er en liste over elementer som er låst av Låsinnstilling i **Innst.**-menyen på kontrollpanelet.

✓: skal låses.

- : Skal ikke låses.

Innst.-meny		Låsinnstilling
Basisinnstillinger		-
	LCD-lysstyrke	-
	Lyder	-
	Innsovingstid	✓
	Strøm av-tidtager	✓
	Direkte strøm på	✓
	Innstillinger dato/kl.	✓
	Språk/Language	✓/-*
	Tastatur (Denne funksjonen kan være utilgjengelig avhengig av region.)	-
	Tidsavbrudd for handling	✓
	PC-tilkobling via USB	✓
Skannerinnstillinger		-
	Sakte	-
	Dobbelmatestopp-timing	✓
	DFDS-funksjon	-
	Papirbeskyttelse	✓
	Oppdagelse av skitt på glasset	✓
	Ultrasonisk registr. av dobbeltmating	✓
	Tidsavbrudd for Modus for automatisk mating	✓
	Bekreft mottaker	✓
Rediger Startskjerm		✓
	Layout	✓
	Legg til ikon	✓
	Fjern ikon	✓
	Flytt ikon	✓
	Gjenopprett standard ikonvisning	✓
Brukerinnstillinger		✓
	Nettverksmappe/FTP	✓
	E-post	✓
	Nettsky	✓
	USB-stasjon	✓


Innst.-meny		Låsinnstilling
Nettverksinnstillinger		✓
	Wi-Fi-oppsett	✓
	Oppsett av kablet LAN	✓
	Nettverkstatus	✓
	Avansert	✓
Web-tjenesteinnstillinger		✓
	Epson Connect-tjenester	✓
Document Capture Pro		-
	Endre innstillinger	✓
Kontaktadministrasjon		-
	Registrer/Slett	✓/-*
	Hyppig	-
	Vis alternativer	-
	Søkealternativer	-
Systemadministrasjon		✓
	Kontaktadministrasjon	✓
	Administratorinnstillinger	✓
	Begrensninger	✓
	Tilgangskontroll	✓
	Passordkryptering	✓
	Kundeforskning	✓
	WSD-innstillinger	✓
	Gjenopprett standardinnst.	✓
	Fastvareoppdatering	✓
Enhetsinformasjon		-

Innst.-meny		Låsinnstilling
	Serienummer	-
	Gjeldende versjon	-
	Sum skanninger	-
	Antall 1-sidige skanninger	-
	Antall 2-sidige skanninger	-
	Antall skanninger med Bæreak	-
	Antall skanninger etter valsbytte	-
	Antall skanninger etter Vanlig rengjøring	-
	Status for godkjenningseenhet	-
	Informasjon om Epson Open Platform	-
	 (Tilbakestill antall skanninger)	✓
Vedlikehold av skanner		-
	Rengjøring av vals	-
	Utskiftning av vedlikeholdsvalse	-
	Tilbakestill antall skanninger	✓
	Slik bytter du den ut	-
	Vanlig rengjøring	-
	Tilbakestill antall skanninger	✓
	Hvordan rengjøre	-
	Glassrengjøring	-
Varselinnstilling for utskiftning av valse		✓
	Antallvarsling	✓
Varslingsinnstillinger for ordinær rengjøring		✓
	Varslingsinnstilling for advarsel	✓
	Antallvarsling	✓

* Du kan angi hvorvidt du vil tillate endringer i **Systemadministrasjon > Begrensninger**.

Logge på som en administrator fra kontrollpanelet



Når **Låsinnstilling** er aktivert kan du bruke hvilken som helst av de følgende metodene til å logge på fra skannerens kontrollpanel.

1. Trykk på  øverst til høyre på skjermen.

2. Når **Velg bruker**-skjermen vises, velger du **Administrator**.

3. Tast inn passordet for å logge inn.

En melding som forteller at pålogging er fullført vises, så vises Hjem-skjermen på kontrollpanelet.

For å logge ut, trykk på  øverst til høyre på skjermen eller trykk på -knappen.

Begrense tilgjengelige funksjoner (Tilgangskontroll)

Du kan begrense brukere ved å registrere brukerkontoer på skanneren.

Når Tilgangskontroll er aktivert, kan brukeren bruke skannefunksjonene ved å angi passordet på skannerens kontrollpanel og logge inn. Du kan ikke skanne hvis du ikke logger inn.

Du kan skanne fra en datamaskin ved å registrere Brukernavn og Passord i skannerdriveren (Epson Scan 2). Se hjelp for Epson Scan 2 eller produktets *Brukerhåndbok* for å finne ut mer om å gjøre innstillingene.

Opprette brukerkontoen

Du kan opprette en Tilgangskontroll-konto.

1. Åpne Web Config og velg **Produktsikkerhet**-fanen > **Innstillinger for tilgangskontroll** > **Brukerinnstillinger**.
2. Klikk på **Legg til** for antallet du vil registrere.



Forsiktighetsregel:

Når du bruker skanneren med et godkjenningssystem fra Epson eller et annet selskap, må du registrere Brukernavn i Innstillinger for tilgangskontroll i spor nummer to til ti.

Programvarer som godkjenningssystemet bruker spor nummer én, slik at brukernavnet ikke vises på skriverens kontrollpanel.

3. Angi hvert element.

Brukernavn:

Skriv inn navnet som vises i brukernavnlisten mellom 1 og 14 tegn langt, med alfanumeriske tegn.

Passord:

Skriv inn et passord på opptil 20 tegn i ASCII (0x20–0x7E). Når passordet initialiseres, lar du det stå tomt.

Velg avkrysningsboksen for å aktivere eller deaktivere hver funksjon.

Velg **Skann** hvis du vil tillate skannefunksjonene.

4. Klikk på **Bruk**.

Redigere brukerkontoen

Du kan redigere den registrerte Tilgangskontroll-kontoen.

1. Åpne Web Config og velg **Produktsikkerhet**-fanen > **Innstillinger for tilgangskontroll** > **Brukerinnstillinger**.
2. Klikk på **Rediger** for antallet du vil redigere.
3. Endre hvert element.
4. Klikk på **Bruk**.

Slette brukerkontoen

Du kan slette den registrerte Tilgangskontroll-kontoen.

1. Åpne Web Config og velg **Produktsikkerhet**-fanen > **Innstillinger for tilgangskontroll** > **Brukerinnstillinger**.
2. Klikk på **Rediger** for antallet du vil slette.
3. Klikk på **Slett**.



Forsiktighetsregel:

Når du klikker på **Slett**, slettes brukerkontoen uten en bekreftelsesmelding. Vær forsiktig når du sletter kontoen.

Aktivere Tilgangskontroll

Når Tilgangskontroll aktiveres, vil bare den registrerte brukeren kunne bruke skanneren.


Merknad:

Når Innstillinger for tilgangskontroll er aktivert, må du varsle brukeren om kontoinformasjonen sin.

1. Åpne Web Config og velg **Produktsikkerhet**-fanen > **Innstillinger for tilgangskontroll** > **Grunnleggende**.
2. Velg **Aktiverer tilgangskontroll**.
Hvis du aktiverer Innstillinger for tilgangskontroll og skanner fra en datamaskin som ikke har godkjenninginformasjon, velger du **Tillat utskrift og skanning uten godkjenninginformasjon fra en datamaskin**.
3. Klikk på **OK**.



Logge på en skanner der Tilgangskontroll er aktivert

Når **Tilgangskontroll** er aktivert kan du bruke hvilken som helst av de følgende metodene til å logge på fra skannerens kontrollpanel.

1. Trykk på  øverst til høyre på skjermen.
2. Når **Velg bruker**-skjermen vises, må du velge brukeren.

3. Tast inn passordet for å logge inn.

En melding som forteller at pålogging er fullført vises, så vises Hjem-skjermen på kontrollpanelet.

For å logge ut, trykk på  øverst til høyre på skjermen eller trykk på -knappen.

Deaktivere eksternt grensesnitt

Du kan deaktivere grensesnittet som brukes for å koble enheten til skanneren. Angi innstillingene for begrensningen for å begrense skanning annet enn via nettverket.

Merknad:

Du kan også angi innstillinger for begrensningen på skannerens kontrollpanel.

PC-tilkobling via USB: **Innst.** > **Basisinnstillinger** > **PC-tilkobling via USB**

1. Gå inn på Web Config og velg **Produktsikkerhet**-fanen > **Eksternt grensesnitt**.

2. Velg **Deaktiver** på funksjonene du vil angi.

Velg **Aktiver** når du vil avbryte kontrollering.

PC-tilkobling via USB

Du kan begrense bruken av USB-forbindelsen fra datamaskinen. Hvis du ønsker å begrense den, velg **Deaktiver**.

3. Klikk på **OK**.

4. Kontroller at den deaktiverte porten ikke kan brukes.

PC-tilkobling via USB

Hvis driveren ble installert på datamaskinen

Koble skanneren til datamaskinen med en USB-kabel, og bekreft at skanneren ikke skanner.

Hvis driveren ikke ble installert på datamaskinen

Windows:

Åpne enhetsbehandling og ikke lukk den igjen, koble skanneren til datamaskinen med en USB-kabel og bekreft at enhetsbehandlerens visning av innhold ikke endres.

Mac OS:

Koble skanneren til datamaskinen med en USB-kabel, og bekreft deretter at du ikke kan legge til skanneren fra **Skrivere og skannere**.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Aktivere programverifisering ved oppstart

Hvis du aktiverer programverifiseringsfunksjonen, kjører skanneren verifisering ved oppstart for å kontrollere om uautoriserte tredjeparter har manipulert programmet. Skanneren starter ikke hvis det oppdages problemer.

Merknad:

Oppstartstiden til skanneren øker når denne funksjonen er aktivert.

1. Åpne Web Config og velg **Produktsikkerhet**-fanen > **Programverifisering ved oppstart**.

Merknad:

Du kan også angi innstillinger for skannerens kontrollpanel.

Innst. > **Systemadministrasjon** > **Programverifisering ved oppstart**

2. Velg **På** for å aktivere **Programverifisering ved oppstart**.
3. Klikk på **OK**.

Deaktivere nettverksskanning fra datamaskinen

Du kan angi følgende innstillinger i Web Config for å deaktivere nettverksskanning med Epson Scan 2 fra datamaskinen din.

1. Åpne Web Config og velg **Skann**-fanen > **Nettverkssøk**.
2. I **Epson Scan 2** tømmer du avmerkingsboksen **Aktiver skanning**.
3. Klikk på **Neste**.
Bekreftelsesskjerm bildet for innstillinger vises.
4. Klikk på **OK**.

Aktivere eller deaktivere WSD-skanning

Merknad:

Du kan også angi innstillinger for skannerens kontrollpanel. Velg **Innst.** > **Systemadministrasjon** > **WSD-innstillinger**.

Du kan aktivere eller deaktivere WSD-skanning.

Hvis du ikke vil at datamaskinen skal konfigurere skanneren som en WSD-skanneenhet, kan du deaktivere WSD-innstillingene.

1. Åpne Web Config og velg **Nettverkssikkerhet**-fanen > **Protokoll**.
2. I **WSD-innstillinger** endrer du avmerkingsboksen **Aktiver WSD**.
3. Klikk på **Neste**.
Bekreftelsesskjerm bildet for innstillinger vises.
4. Klikk på **OK**.

Merknad:

Hvis datamaskinen din fortsatt konfigurerer skanneren som en WSD-skanneenhet, må du velge **Skann**-fanen > **Nettverkssøk** og deretter tømme armerkingsboksen **Aktiver skanning** i **AirPrint**.

Hvis **AirPrint** er deaktivert, er **Mopria-skanning** fra **Chromebook** og **Windows** og **Mopria Scan**-appen også deaktivert.

Administrere en ekstern skanner

Sjekk informasjon for en ekstern skanner

Du kan kontrollere følgende informasjon om skanneren fra **Status** ved å bruke Web Config.

Produktets status

Sjekk status, skytjeneste, produktnummer, MAC-adresse, osv.

Nettverkstatus

Sjekk informasjon om status for nettverkstilkobling, IP-adresse, DNS-server, osv.

Bruksstatus

Sjekk første dags skanninger, skanningsteller, osv.

Maskinvarestatus

Sjekk statusen til hver av skannerens funksjoner.

Paneløyeblikksbilde

Viser et øyeblikksbilde av skjermen som vises på skannerens kontrollpanel.

Motta e-postvarslinger når det skjer hendelser

Om e-postvarsler

Dette er varslingsfunksjonen som, når hendelser som skannestopp og skannerfeil oppstår, sender e-posten til den angitte adressen.

Du kan registrere opptil fem destinasjoner og angi varslingsinnstillingene for hver destinasjon.

For å bruke denne funksjonen, må du konfigurere e-postserveren før du konfigurerer varslinger.

Relatert informasjon

➔ [“Registrere en e-postserver” på side 44](#)

Konfigurere e-postvarsel

Konfigurer e-postvarsel ved hjelp av Web Config.

1. Gå inn på Web Config og velg **Enhetsadministrasjon**-fanen > **E-postvarsling**.

2. Angi emnet for e-postvarsling.

Velg innholdet som vises på emnet fra de to nedtrekkslistene.

Det valgte innholdet vises ved siden av **Emne**.

Det samme innholdet kan angis til venstre og høyre.

Når antall tegn i **Sted** overskrider 32 bytes, utelates de overskridende tegnene.

3. Skriv inn e-postadressen som skal sende e-postvarslingen.

Bruk A–Z a–z 0–9 ! # \$ % & ' * + - . / = ? ^ _ { | } ~ @, og skriv inn mellom 1 og 255 tegn.

4. Velg språk for e-postvarsler.

5. Velg avkrysningsboksen på hendelsen du ønsker å motta varsling for.

Antall **Varslingsinnstillinger** er knyttet til destinasjonsantallet for **E-postadresseinnstillinger**.

Eksempel:

Hvis du ønsker å sende et varsel til e-postadressen som er angitt for nummer 1 i **E-postadresseinnstillinger**, når administratorpassordet er endret, velger du avmerkingsboksen for kolonne **1** i linjen

Administratorpassord endret.

6. Klikk på **OK**.

Bekreft at en e-postvarsling vil bli sendt ved å forårsake en hendelse.

Eksempel: Administratorpassordet har blitt endret.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Elementer for e-postvarsling

Artikler	Innstillinger og forklaring
Administratorpassord endret	Varsler når administratorpassordet har blitt endret.
Skannerfeil	Varsler når det har oppstått skannerfeil.
Wi-Fi-feil	Varsler når det har oppstått feil med det trådløse LAN-grensesnittet.

Bruke Web Config til å kontrollere skannerens strømforsyning

Hvis datamaskinen er ekstern fra skanneren, kan du fortsatt bruke Web Config til å slå av eller starte skanneren på nytt.

1. Åpne Web Config og velg **Enhetsadministrasjon**-fanen > **Av/på**.
2. Velg **Slå av** eller **Start på nytt**.
3. Klikk på **Utfør**.

Gjenopprette standardinnstillingene

Du kan velge nettverksinnstillingene eller andre innstillinger som er lagret på skanneren, for å gjenopprette dem til standardinnstillingene.

1. Åpne Web Config og velg **Enhetsadministrasjon**-fanen > **Gjenopprett standardinnstillinger**.

Merknad:

Du kan også angi innstillinger for skannerens kontrollpanel.

Innst. > **Systemadministrasjon** > **Gjenopprett standardinnst.**

2. Velg elementene du vil gjenopprette.

3. Klikk på **Utfør**.

Til slutt følger du instruksjonene på skjermen.

Informasjon om Epson Remote Services

Epson Remote Services er en tjeneste som med jevne mellomrom henter skannerinformasjon over internett. Denne kan brukes til å forutse når forbruksvarer og erstatningsdeler må erstattes eller trenger påfyll, og for å løse feilmeldinger eller problemer raskt.

Kontakt forhandleren for mer informasjon om Epson Remote Services.

Problemløsning

Glemt administratorpassordet ditt

Du trenger hjelp fra servicepersonell. Kontakt lokalforhandleren.

Merknad:

Følgende gir opprinnelige verdier for Web Config-administratoren.

Brukernavn: ingen (tomt)

Passord: avhenger av etiketten på produktet.

Hvis det er en PASSWORD-etikett på baksiden, angir du det 8-sifrede nummeret på etiketten.

Hvis det ikke er en PASSWORD-etikett der, angir du serienummeret på etiketten på baksiden av produktet som administratorpassord den første gangen.

Hvis du gjenoppretter administratorpassordet, tilbakestilles det til passordet som var satt opp på kjøpstidspunktet.

Avanserte sikkerhetsinnstillinger

Sikkerhetsinnstillinger og forebygging av farlige situasjoner.	88
Kontrollere med protokoller.	89
Bruke et digitalt sertifikat.	92
SSL/TLS-kommunikasjon med skanneren.	97
Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering.	98
Koble skanneren til et IEEE802.1X-nettverk.	109
Løse problemer med avanserte sikkerhetsinnstillinger.	111

Sikkerhetsinnstillinger og forebygging av farlige situasjoner

Når en skanner er koblet til et nettverk, kan du få tilgang til den eksternt. I tillegg kan flere personer dele skanneren, noe som er nyttig for å øke effektiviteten av driften og gi økt bekvemmelighet. Imidlertid økes risikoen for ulovlig tilgang, ulovlig bruk og manipulering av data. Hvis du bruker skanneren i et miljø hvor det er tilgang til Internett, er risikoen enda høyere.

For skannere som ikke har eksternt tilgangsbeskyttelse vil det være mulig å lese historikk for kontakter som er lagret i skanneren via Internett.

For å unngå denne risikoen tilbyr Epson-skanner en rekke ulike sikkerhetsteknologier.

Still inn skanneren etter behov i henhold til de miljøforhold som har blitt bygget etter kundens miljøinformasjon.

Navn	Funksjonstype	Hva skal stilles inn	Hva skal forebygges
Kontroll av protokoller	Styrer protokollene og tjenestene som skal brukes til kommunikasjon mellom skannere og datamaskiner, og aktiverer og deaktiverer funksjoner.	En protokoll eller en tjeneste som brukes til funksjoner som tillatt eller forbudt separat.	Reduserer sikkerhetsrisikoer som kan oppstå ved utilsiktet bruk ved å hindre brukere fra å bruke unødvendige funksjoner.
SSL/TLS-kommunikasjon	Kommunikasjonsinnholdet er kryptert med SSL/TLS-kommunikasjon ved tilgang til Epson-serveren via Internett fra skanneren, som kommuniserer til datamaskinen via nettleseren ved hjelp av Epson Connect og oppdatering av fastvare.	Få tak i et CA-signert sertifikat, og deretter importer det til skanneren.	Fjerning av en identifikasjon for skanneren gjennom CA-signerte sertifikater forhindrer etterligning og uautorisert tilgang. I tillegg er kommunikasjonsinnholdet SSL/TLS-beskyttet, noe som forhindrer lekkasje av innholdet for skannedata og installasjonsdata.
IPsec/IP-filtrering	Du kan stille inn til å tillate brudd og avkutting av data som er fra en bestemt klient eller en bestemt type. Siden IPsec beskytter dataene etter IP-pakkeenhet (kryptering og autentisering), kan du trygt kommunisere usikret protokoll.	Opprett grunnleggende retningslinjer og individuelle retningslinjer for å angi hvilke klienter eller datatyper som kan få tilgang til skanneren.	Beskytt mot uautorisert tilgang og tukling og avskjæring av kommunikasjonsdata til skanneren.
IEEE 802.1X	Tillater kun godkjente brukere å koble til nettverket. Tillater kun at en bruker med godkjenning bruker skanneren.	Godkjenningsinnstilling av RADIUS-serveren (godkjenningsserver).	Beskytt mot uautorisert tilgang og bruk av skanneren.

Relatert informasjon

- ➔ [“Kontrollere med protokoller” på side 89](#)
- ➔ [“SSL/TLS-kommunikasjon med skanneren” på side 97](#)
- ➔ [“Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering” på side 98](#)
- ➔ [“Koble skanneren til et IEEE802.1X-nettverk” på side 109](#)

Innstilling av sikkerhetsfunksjoner

Ved innstilling av IPsec/IP-filtrering eller IEEE 802.1X, anbefales det at du går inn på Web Config med SSL/TLS for å kommunisere innstillingsinformasjon for å redusere faren for sikkerhetsbrudd slik som manipulering eller avskjæring.

Forsikre at du konfigurerer administratorpassordet før du angir IPsec/IP-filtrering eller IEEE 802.1X.

Kontrollere med protokoller

Du kan skanne via ulike baner og protokoller. Du kan også bruke nettverkskanning fra et uspesifisert antall datamaskiner i nettverket.

Du kan redusere utilsiktede sikkerhetsrisikoer ved å begrense skanning via bestemte baner eller ved å kontrollere de tilgjengelige funksjonene.

Kontrollprotokoller

Konfigurer protokollinnstillingene som støttes av skanneren.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet** tab > **Protokoll**.
2. Konfigurer hvert element.
3. Klikk på **Neste**.
4. Klikk på **OK**.
Innstillingene brukes på skanneren.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Protokoller du kan Aktivere eller Deaktivere

Protokoll	Beskrivelse
Bonjour-innstillinger	Du kan angi om du vil bruke Bonjour. Bonjour brukes til å søke etter enheter, skanne, og så videre.
SLP-innstillinger	Du kan aktivere eller deaktivere SLP-funksjonen. SLP brukes for push-skanning og nettverkssøk i EpsonNet Config.
WSD-innstillinger	Du kan aktivere eller deaktivere WSD-funksjonen. Når denne er aktivert, kan du legge til WSD-enheter og skanne fra WSD-porten.
LLTD-innstillinger	Du kan aktivere eller deaktivere LLTD-funksjonen. Når denne er aktivert, vises den på nettverkskartet i Windows.
LLMNR-innstillinger	Du kan aktivere eller deaktivere LLMNR-funksjonen. Når denne er aktivert, kan du bruke navneløsning uten NetBIOS selv om du ikke kan bruke DNS.

Protokoll	Beskrivelse
SNMPv1/v2c-innstillinger	Du kan angi om du vil aktivere SNMPv1/v2c. Dette brukes til å sette opp enheter, overvåking og så videre.
SNMPv3-innstillinger	Du kan angi om du vil aktivere SNMPv3. Dette brukes til å sette opp krypterte enheter, overvåking, osv.

Innstillingselementer for protokoll

Bonjour-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Bruk Bonjour	Marker her for å søke etter eller bruke enheter via Bonjour.
Bonjour-navn	Viser Bonjour-navn.
Bonjour servicenavn	Viser Bonjour-tjenestenavn.
Sted	Viser Bonjour-plasseringsnavn.
Wide-Area Bonjour	Angi hvorvidt Wide-Area Bonjour skal brukes.

SLP-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver SLP	Velg dette for å aktivere SLP-funksjonen. Dette brukes som nettverkssøk i EpsonNet Config.

WSD-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver WSD	Velg dette for å aktivere tillegging av enheter med WSD og skann fra WSD-porten.
Tidsavbrudd for skanning (sek)	Skriv inn verdi for tidsavbrudd av kommunikasjon for WSD-skanning mellom 3 og 3600 sekunder.
Enhetsnavn	Viser WSD-enhetsnavn.
Sted	Viser WSD-plasseringsnavn.

LLTD-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver LLTD	Velg dette for å aktivere LLTD. Skanneren vises på Windows-nettverkskartet.
Enhetsnavn	Viser LLTD-enhetsnavn.

LLMNR-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver LLMNR	Velg dette for å aktivere LLMNR. Du kan bruke navneløsning uten NetBIOS selv om du ikke kan bruke DNS.

SNMPv1/v2c-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver SNMPv1/v2c	Velg for å aktivere SNMPv1/v2c.
Tilgangsautoritet	Definer tilgangsrettigheter når SNMPv1/v2c er aktivert. Velg Skrivebeskyttet eller Les/Skriv .
Gruppenavn (skrivebeskyttet)	Skriv inn 0 til 32 ASCII-tegn (0x20 til 0x7E).
Gruppenavn (lese/skrive)	Skriv inn 0 til 32 ASCII-tegn (0x20 til 0x7E).

SNMPv3-innstillinger

Artikler	Innstillingsverdi og beskrivelse
Aktiver SNMPv3	SNMPv3 er aktivert når boksen er krysset av.
Brukernavn	Skriv inn mellom 1 og 32 tegn ved hjelp av 1-biters tegn.
Godkjenningsinnstillinger	
Algoritme	Velg en alorytme for autentisering for SNMPv3.
Passord	Velg et passord for autentisering for SNMPv3. Skriv inn mellom 8 og 32 tegn i ASCII (0x20–0x7E). Hvis du ikke angir dette, la det stå tomt.
Bekreft passord	Skriv inn passordet du konfigurerte som bekreftelse.
Krypteringsinnstillinger	
Algoritme	Velg en alorytme for kryptering for SNMPv3.
Passord	Velg et passord for kryptering for SNMPv3. Skriv inn mellom 8 og 32 tegn i ASCII (0x20–0x7E). Hvis du ikke angir dette, la det stå tomt.
Bekreft passord	Skriv inn passordet du konfigurerte som bekreftelse.
Kontekstnavn	Skriv inn maksimalt 32 tegn i Unicode (UTF-8). Hvis du ikke angir dette, la det stå tomt. Antall tegn som kan angis varierer avhengig av språket som er brukt.

Bruke et digitalt sertifikat

Om digital sertifisering

CA-signert sertifikat

Dette sertifikatet er signert av CA (sertifiseringsinstans). Du kan få det ved å søke til sertifiseringsinstansen. Dette sertifikatet sertifiserer skannerens eksistens og brukes for SSL/TLS-kommunikasjon, slik at du kan påse at datakommunikasjonen er sikker.

Når dette brukes for SSL/TLS-kommunikasjon, brukes det som et serversertifikat.

Når det er angitt til kommunikasjon med IPsec/IP-filtrering eller IEEE 802.1X, brukes det som et klientsertifikat.

CA-sertifikat

Dette er et sertifikat i kjeden av CA-signert sertifikat, også kalt det mellomliggende CA-sertifikatet. Det brukes av nettleseren til å validere banen til skannerens sertifikat når du åpner serveren til den andre parten eller Web Config.

For CA-sertifikatet, angi når validering skal gjennomføres for banen til serversertifikat som åpnes fra skanneren. For skanneren, angi til å sertifisere banen til CA-signert sertifikat for SSL/TLS-tilkobling.

Du kan få skannerens CA-sertifikat fra sertifiseringsinstansen hvor CA-sertifikatet ble utstedt.

Du kan også få CA-sertifikatet brukt til å validere den andre partens server fra sertifiseringsinstansen som utstedte CA-signert sertifikat til den andre serveren.

Selvsignert sertifikat

Dette er et sertifikat som skanneren signerer og til utsteder selv. Det kalles også rotsertifikatet. Ettersom utstederen sertifiserer selv, er det ikke pålitelig og kan ikke forhindre falske identiteter.

Bruk det når sikkerhetsinnstilling angis og når enkel SSL/TLS-kommunikasjon utføres uten CA-signert sertifikat.

Hvis du bruker dette sertifikatet som SSL/TLS-kommunikasjon, kan det vises en sikkerhetsadvarsel i nettleseren ettersom sertifikatet ikke er registrert på en nettleseren. Du kan bare bruke Selvsignert sertifikat for SSL/TLS-kommunikasjon.

Relatert informasjon

- ➔ [“Konfigurere et CA-signert sertifikat” på side 92](#)
- ➔ [“Oppdatere et selvsignert sertifikat” på side 96](#)
- ➔ [“Konfigurere et CA-sertifikat” på side 96](#)

Konfigurere et CA-signert sertifikat

Hente et CA-signert sertifikat

Vil du hente et CA-signert sertifikat, oppretter du en CSR (forespørsel om sertifikatsignering) og sender den til sertifiseringsinstansen. Du kan opprette en CSR ved hjelp av Web Config og en datamaskin.

Følg trinnene for å opprette en CSR og hente et CA-signert sertifikat med Web Config. Når du oppretter en CSR med Web Config, får sertifikatet PEM/DER-format.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen. Deretter velger du **SSL/TLS > Sertifikat**, eller **IPsec/IP-filtrering > Klientsertifikat** eller **IEEE802.1X > Klientsertifikat**.

Uansett hva du velger, kan du få samme sertifikat og bruke det i felles.

2. Klikk **Generer** under **CSR**.

Det åpnes en side for oppretting av CSR.

3. Angi en verdi for hvert element.

Merknad:

Tilgjengelig nøkkellengde og forkortelser varierer etter sertifiseringsinstans. Opprett en forespørsel i henhold til reglene for hver sertifiseringsinstans.

4. Klikk på **OK**.

Det vises en fullføringsmelding.

5. Velg kategorien **Nettverkssikkerhet**. Deretter velger du **SSL/TLS > Sertifikat**, eller **IPsec/IP-filtrering > Klientsertifikat** eller **IEEE802.1X > Klientsertifikat**.

6. Klikk én av nedlastingsknappene under **CSR** i henhold til angitt format for hver sertifiseringsinstans for å laste ned en CSR til datamaskinen.



Forsiktighetsregel:

Ikke generer CSR på nytt. Hvis du gjør det, kan du ikke være i stand til å importere et utstedt CA-signert sertifikat.

7. Send CSR-en til en sertifiseringsinstans, og hent et CA-signert sertifikat.

Følg reglene til hver sertifiseringsinstans når det gjelder sendemetode og format.

8. Lagre utstedt CA-signert sertifikat på en datamaskin som er koblet til skanneren.

Henting av et CA-signert sertifikat er fullført når du lagrer sertifikatet et sted.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Innstillingselementer for CSR

Artikler	Innstillinger og forklaring
Nøkkellengde	Velg en nøkkellengde for en CSR.
Vanlig navn	<p>Du kan skrive inn mellom 1 og 128 tegn. Hvis dette er en IP-adresse, bør det være en statisk IP-adresse. Du kan skrive inn fra 1 til 5 IPv4-adresser, IPv6-adresser, vertsnavn og FQDN-er ved å separere dem med komma.</p> <p>Det første elementet lagres til fellesnavnet, og andre elementer lagres til aliasfeltet til sertifikatsemnet.</p> <p>Eksempel:</p> <p>Skannerens IP-adresse: 192.0.2.123, Skannernavn: EPSONA1B2C3</p> <p>Vanlig navn: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123</p>

Artikler	Innstillinger og forklaring
Organisasjon/ Organisasjonsenhet/ Beliggenhet/ Stat/provins	Du kan skrive inn mellom 0 og 64 tegn i ASCII (0x20–0x7E). Du kan skille forskjellige navn med komma.
Land	Skriv inn en tosfret landskode angitt av ISO-3166.
Avsenderens e-postadresse	Du kan skrive inn mottakers e-postadresse i innstillingene for e-postserveren. Skriv inn samme e-postadresse som Avsenderens e-postadresse for Nettverk-fanen > E-postserver > Grunnleggende .

Importere et CA-signert sertifikat

Importer det hentede CA-signert sertifikat til skanneren.



Forsiktighetsregel:

- Kontroller at skannerens dato og klokkeslett er riktig innstilt. Sertifikatet kan være ugyldig.
- Hvis du henter et sertifikat med en CSR som er opprettet fra Web Config, kan du importere et sertifikat én gang.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen. Deretter velger du **SSL/TLS > Sertifikat**, eller **IPsec/IP-filtrering > Klientsertifikat** eller **IEEE802.1X > Klientsertifikat**.

2. Klikk **Importer**

Det åpnes en side for import av sertifikatet.

3. Angi en verdi for hvert element. Angi **CA-sertifikat 1** og **CA-sertifikat 2** ved verifisering av sertifikatets bane på nettleseren som har tilgang til skanneren.

Avhengig av hvor du oppretter CSR og filformatet til sertifikatet, kan påkrevde innstillingselementer variere. Skriv inn verdier for påkrevde elementer i henhold til følgende.

- Et sertifikat med PEM/DER-format som er hentet fra Web Config
 - Privat nøkkel:** Må ikke konfigureres fordi skanneren inneholder en privattast.
 - Passord:** Skal ikke konfigureres.
 - CA-sertifikat 1/CA-sertifikat 2:** Valgfritt
- Et sertifikat med PEM/DER-format som er hentet fra datamaskinen
 - Privat nøkkel:** Må angis.
 - Passord:** Skal ikke konfigureres.
 - CA-sertifikat 1/CA-sertifikat 2:** Valgfritt
- Et sertifikat med PKCS#12-format som er hentet fra datamaskinen
 - Privat nøkkel:** Skal ikke konfigureres.
 - Passord:** Valgfritt
 - CA-sertifikat 1/CA-sertifikat 2:** Skal ikke konfigureres.

4. Klikk på **OK**.

Det vises en fullføringsmelding.

Merknad:

Klikk **Bekreft** for å bekrefte sertifikatinformasjonen.

Relatert informasjon

➔ “Slik kjører du Web Config i en nettleser” på side 37

Innstillingselementer for import av CA-signert sertifikat

Artikler	Innstillinger og forklaring
Serversertifikat eller Klientsertifikat	Velg format for sertifikatet. For SSL/TLS-tilkobling vises Serversertifikat. For IPsec-/IP-filtrering eller IEEE 802.1X vises Klientsertifikat.
Privat nøkkel	Hvis du henter et sertifikat med PEM/DER-format med en CSR som er opprettet fra en datamaskin, angi du filen for privatnøkkelen som samsvarer med sertifikatet.
Passord	Hvis filformatet er Sertifikat med privat nøkkel (PKCS#12) , skriver du inn passordet for kryptering av den private nøkkelen som er angitt når du henter sertifikatet.
CA-sertifikat 1	Hvis sertifikatets format er Sertifikat (PEM/DER) , importerer du et sertifikat fra en CA-signert sertifikat som brukes som utsteder av serversertifikater. Angi en fil om nødvendig.
CA-sertifikat 2	Hvis sertifikatets format er Sertifikat (PEM/DER) , importerer du et sertifikat fra en sertifiseringsinstans som utsteder CA-sertifikat 1. Angi en fil om nødvendig.

Slette et CA-signert sertifikat

Du kan slette et importert sertifikat når sertifikatet er utløpt eller når en kryptert tilkobling ikke lenger er nødvendig.



Forsiktighetsregel:

Hvis du henter et sertifikat med en CSR som er opprettet fra Web Config, kan du ikke importere et slettet sertifikat på nytt. I så fall må du opprette en CSR og hente et sertifikat på nytt.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen. Deretter velger du **SSL/TLS > Sertifikat**, eller **IPsec/IP-filtrering > Klientsertifikat** eller **IEEE802.1X > Klientsertifikat**.
2. Klikk på **Slett**.
3. Bekreft at du vil slette sertifikatet i meldingen som vises.

Relatert informasjon

➔ “Slik kjører du Web Config i en nettleser” på side 37

Oppdatere et selvsignert sertifikat

Ettersom Selvsignert sertifikat utstedes av skanneren, kan du oppdatere det når det har utløpt eller når innholdsbeskrivelsen endres.

1. Gå inn på Web Config og velg **Nettverkssikkerhet** tab > **SSL/TLS** > **Sertifikat**.
2. Klikk på **Oppdater**.
3. Skriv inn **Vanlig navn**.

Du kan skrive inn opptil 5 IPv4-adresser, IPv6-adresser, vertsnavn og FQDN-er mellom 1 og 128 tegn og separere dem med komma. Den første parameteren lagres til fellesnavnet, og de andre lagres til aliasfeltet for emnet til sertifikatet.

Eksempel:

Skannerens IP-adresse: 192.0.2.123, Skannernavn: EPSONA1B2C3

Fellesnavn: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123

4. Angi en gyldighetsperiode for sertifikatet.
5. Klikk på **Neste**.
6. Klikk på **OK**.

Det vises en bekreftelsesmelding.

Skanneren er oppdatert.

Merknad:

Du kan kontrollere sertifikatinformasjonen fra **Nettverkssikkerhet**-fanen > **SSL/TLS** > **Sertifikat** > **Selvsignert sertifikat** og klikk på **Bekreft**.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Konfigurere et CA-sertifikat

Når du angir CA-sertifikat, kan du validere banen til serverens CA-sertifikat som brukes av skanneren. Dette kan forhindre falske identiteter.

Du kan få CA-sertifikat fra sertifiseringsinstansen hvor CA-signert sertifikat ble utstedt.

Importere et CA-sertifikat

Importer CA-sertifikat til skanneren.

1. Åpne Web Config og velg **Nettverkssikkerhet**-fanen > **CA-sertifikat**.
2. Klikk på **Importer**.
3. Velg CA-sertifikat du vil importere.
4. Klikk på **OK**.

Når importeringen er fullført, sendes du tilbake til **CA-sertifikat** skjermen, og importert CA-sertifikat vises.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Slette et CA-sertifikat

Du kan slette et importert CA-sertifikat.

1. Gå inn på Web Config og velg deretter **Nettverkssikkerhet**-fanen > **CA-sertifikat**.
2. Klikk på **Slett** ved siden av CA-sertifikat du vil slette.
3. Bekreft at du vil slette sertifikatet i meldingen som vises.
4. Klikk på **Start nettverk på nytt** og kontroller at det slettede CA-sertifikatet ikke er oppført i det oppdaterte skjermbildet.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

SSL/TLS-kommunikasjon med skanneren

Når skiversertifikatet angis ved bruk av SSL/TLS (Secure Sockets Layer/Transport Layer Security)-kommunikasjon med skanneren kan du kryptere kommunikasjonsbanen mellom datamaskinene. Gjør dette dersom du ønsker å forhindre ekstern eller uautorisert tilgang.

Konfigurere grunnleggende SSL/TLS-innstillinger

Hvis skanneren støtter HTTPS-serverfunksjonen, kan du bruke SSL/TLS-kommunikasjon til å kryptere kommunikasjon. Du kan konfigurere og styre skanneren med Web Config på en sikker måte.

Konfigurer krypteringsstyrke og funksjon for videresending.

1. Gå inn på Web Config og velg **Nettverkssikkerhet**-fanen > **SSL/TLS** > **Grunnleggende**.
2. Velg en verdi for hvert element.
 - Krypteringsstyrke
Velg nivå for krypteringsstyrke.
 - Omdiriger HTTP til HTTPS
Omdirigering til HTTPS når HTTP åpnes.
3. Klikk på **Neste**.
Det vises en bekreftelsesmelding.

4. Klikk på **OK**.
Skanneren er oppdatert.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Konfigurere et serversertifikat for skanneren

1. Gå inn på Web Config og velg **Nettverkssikkerhet**-fanen > **SSL/TLS** > **Sertifikat**.
2. Angi sertifikatet som skal brukes på **Serversertifikat**.
 - Selvsignert sertifikat
Det er generert et selvsignert sertifikat av skanneren. Velg dette hvis du ikke henter et CA-signert sertifikat.
 - CA-signert sertifikat
Hvis du har hentet og importert et CA-signert sertifikat på forhånd, kan du angi dette.
3. Klikk på **Neste**.
Det vises en bekreftelsesmelding.
4. Klikk på **OK**.
Skanneren er oppdatert.

Relatert informasjon

- ➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)
- ➔ [“Konfigurere et CA-signert sertifikat” på side 92](#)
- ➔ [“Konfigurere et CA-sertifikat” på side 96](#)

Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering

Om IPsec/IP-filtrering

Du kan filtrere trafikk basert på IP-adresser, tjenester og port ved å bruke IPsec/IP-filtreringsfunksjon. Ved å kombinere filtreringen kan du konfigurere skanneren til å godta eller blokkere bestemte klienter og bestemte data. Du kan dessuten øke sikkerhetsnivået ved hjelp av IPsec.

Merknad:

Datamaskiner som kjører Windows Vista eller senere, eller Windows Server 2008 eller senere støtter IPsec.

Konfigurere standardpolicy

Vil du filtrere trafikk, kan du konfigurere standardpolicyen. Standardpolicyen gjelder for alle brukere eller grupper som kobler til skanneren. Du kan konfigurere gruppepolicyer hvis du vil ha mer detaljert kontroll over brukere og brukergrupper.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende**.
2. Angi en verdi for hvert element.
3. Klikk på **Neste**.
Det vises en bekreftelsesmelding.
4. Klikk på **OK**.
Skanneren er oppdatert.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser”](#) på side 37

Innstillingselementer for Standardpolicy

Standardpolicy

Artikler	Innstillinger og forklaring
IPsec/IP-filtrering	Du kan aktivere eller deaktivere en funksjon for IPsec-/IP-filtrering.

Tilgangskontroll

Konfigurer en kontrollmetode for trafikk av IP-pakker.

Artikler	Innstillinger og forklaring
Gi tilgang	Velg dette for å tillate at konfigurerte IP-pakker passerer.
Nekt tilgang	Velg dette for å hindre at konfigurerte IP-pakker passerer.
IPsec	Velg dette for å tillate at konfigurerte IPsec-pakker passerer.

IKE-versjon

Velg **IKEv1** eller **IKEv2** for **IKE-versjon**. Velg en av dem avhengig av hvilken enhet skanneren er koblet til.

IKEv1

Følgende elementer vises når du velger **IKEv1** for **IKE-versjon**.

Artikler	Innstillinger og forklaring
Godkjenning metode	Vil du velge Sertifikat , må du på forhånd hente og importere et CA-signert sertifikat.
Forhåndsdelte nøkkel	Hvis du velger Forhåndsdelte nøkkel for Godkjenning metode , skriver du inn en forhåndsdelte tast på opptil 127 tegn.
Bekreft Forhåndsdelte nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.

IKEv2

Følgende elementer vises når du velger **IKEv2** for **IKE-versjon**.

Artikler	Innstillinger og forklaring	
Lokal	Godkjenning metode	Vil du velge Sertifikat , må du på forhånd hente og importere et CA-signert sertifikat.
	ID-type	Hvis du velger Forhåndsdelte nøkkel som Godkjenning metode , må du velge ID-typen for skanneren.
	ID	Angi skannerens ID, som samsvarer med ID-typen. Du kan ikke bruke «@», «#» eller «=>» som første tegn. Unikt navn: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «=>». IP-adresse: Angi format, enten IPv4 eller IPv6. FQDN: Skriv inn en kombinasjon av mellom 1 og 255 tegn med A–Z, a–z, 0–9, «-», og punktum (.). E-postadresse: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «@». Nøkkel-ID: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Forhåndsdelte nøkkel	Hvis du velger Forhåndsdelte nøkkel for Godkjenning metode , skriver du inn en forhåndsdelte tast på opptil 127 tegn.
	Bekreft Forhåndsdelte nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.

Artikler		Innstillinger og forklaring
Ekstern	Godkjenningstype	Vil du velge Sertifikat , må du på forhånd hente og importere et CA-signert sertifikat.
	ID-type	Hvis du velger Forhåndsdelte nøkler som Godkjenningstype , må du velge ID-type for enheten du vil godkjenne.
	ID	Angi skannerens ID, som samsvarer med ID-type. Du kan ikke bruke «@», «#» eller «=» som første tegn. Unikt navn: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «=». IP-adresse: Angi format, enten IPv4 eller IPv6. FQDN: Skriv inn en kombinasjon av mellom 1 og 255 tegn med A–Z, a–z, 0–9, «-», og punktum (.). E-postadresse: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «@». Nøkkel-ID: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Forhåndsdelte nøkler	Hvis du velger Forhåndsdelte nøkler for Godkjenningstype , skriver du inn en forhåndsdelte tast på opptil 127 tegn.
	Bekreft Forhåndsdelte nøkler	Skriv inn tasten du konfigurerte for bekreftelse.

Innkapsling

Velger du **IPsec** for **Tilgangskontroll**, må du konfigurere en innkapslingsmodus.

Artikler	Innstillinger og forklaring
Transportmodus	Velg dette hvis du bare bruker skanneren på samme LAN. IP-pakker med lag 4 eller nyere blir kryptert.
Tunnelmodus	Hvis du bruker skanneren på et nettverk som kan kobles til Internett, slik som IPsec-VPN, velg dette alternativet. Toppteksten og dataene i IP-pakkene blir kryptert. Ekstern gateway (Tunnelmodus): Hvis du velger Tunnelmodus for Innkapsling , skriver du inn en gateway-adresse på mellom 1 og 39 tegn.

Sikkerhetsprotokoll

Velg et alternativ hvis du velger **IPsec** for **Tilgangskontroll**.

Artikler	Innstillinger og forklaring
ESP	Velg dette for å sikre integriteten til en godkjenning og dataene, samt kryptere data.
AH	Velg dette for å sikre integriteten til en godkjenning og dataene. Du kan bruke IPsec selv om det er forbudt å kryptere data.

❑ Algoritmeinnstillinger

Det anbefales at du velger **Enhver** for alle innstillinger, eller velger et annet element enn **Enhver** for hver innstilling. Hvis du velger **Enhver** for enkelte innstillinger, og velger et annet element enn **Enhver** for de andre innstillingene, kan enheten muligens ikke kommunisere, avhengig av den andre enheten du vil godkjenne.

Artikler		Innstillinger og forklaring
IKE	Kryptering	Velg krypteringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
	Godkjenning	Velg godkjenningalgoritme for IKE.
	Nøkkelutveksling	Velg nøkkeldringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
ESP	Kryptering	Velg krypteringsalgoritme for ESP. Dette er tilgjengelig når ESP er valgt for Sikkerhetsprotokoll .
	Godkjenning	Velg godkjenningalgoritme for ESP. Dette er tilgjengelig når ESP er valgt for Sikkerhetsprotokoll .
AH	Godkjenning	Velg krypteringsalgoritme for AH. Dette er tilgjengelig når AH er valgt for Sikkerhetsprotokoll .

Konfigurere gruppepolicy

En gruppepolicy er én eller flere regler som brukes på en bruker eller brukergruppe. Skanneren kontrollerer IP-pakker som samsvarer med konfigurerte policyer. IP-pakker godkjennes i rekkefølge som gruppepolicy 1 til 10, og deretter som standardpolicy.

- Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende**.
- Klikk på en numerert tast du vil konfigurere.
- Angi en verdi for hvert element.
- Klikk på **Neste**.
Det vises en bekreftelsesmelding.
- Klikk på **OK**.
Skanneren er oppdatert.

Innstillingselementer for Gruppepolicy

Artikler	Innstillinger og forklaring
Deaktiver denne Gruppepolicy	Du kan aktivere eller deaktivere en gruppepolicy.

Tilgangskontroll

Konfigurer en kontrollmetode for trafikk av IP-pakker.

Artikler	Innstillinger og forklaring
Gi tilgang	Velg dette for å tillate at konfigurerte IP-pakker passerer.
Nekt tilgang	Velg dette for å hindre at konfigurerte IP-pakker passerer.
IPsec	Velg dette for å tillate at konfigurerte IPsec-pakker passerer.

Lokal adresse (skanner)

Velg en IPv4-adresse eller IPv6-adresse som matcher ditt nettverksmiljø. Hvis en IP-adresse er gitt automatisk, kan du velge **Bruk automatisk innhentet IPv4-adresse**.

Merknad:

Hvis en IPv6-adresse tilordnes automatisk, kan tilkoblingen være utilgjengelig. Konfigurer en statisk IPv6-adresse.

Ekstern adresse (vert)

Skriv inn en enhets IP-adresse for å kontrollere tilgangen. IP-adressen må være mindre enn 43 tegn. Hvis du ikke skriver inn en IP-adresse, blir alle adressene kontrollerte.

Merknad:

Hvis en IP-adresse tilordnes automatisk (f.eks. tilordnes via DHCP), kan tilkoblingen være utilgjengelig. Konfigurer en statisk IP-adresse.

Metode for å velge port

Velg en metode for å spesifisere porter.

- Tjenestenaavn

Velg et alternativ hvis du velger **Tjenestenaavn** for **Metode for å velge port**.

- Transportprotokoll

Velger du **Portnummer** for **Metode for å velge port**, må du konfigurere en innkapslingsmodus.

Artikler	Innstillinger og forklaring
Alle protokoller	Velg dette for å kontrollere alle protokolltyper.
TCP	Velg dette for å kontrollere data for unikasting.
UDP	Velg dette for å kontrollere data for kringkasting og multikasting.
ICMPv4	Velg dette for å kontrollere Ping-kommando.

- Lokal port

Hvis du velger **Portnummer** for **Metode for å velge port** og hvis du velger **TCP** eller **UDP** for **Transportprotokoll**, skriv inn portnumre for å kontrollere mottakspakker, og separer dem med kommaer. Du kan skrive inn opptil 10 portnumre.

Eksempel: 20,80,119,5220

Hvis du ikke skriver inn et portnummer, blir alle portene kontrollert.

- Ekstern port

Hvis du velger **Portnummer** for **Metode for å velge port** og hvis du velger **TCP** eller **UDP** for **Transportprotokoll**, skriv inn portnumre for å kontrollere sendingspakker, og separer dem med kommaer. Du kan skrive inn opptil 10 portnumre.

Eksempel: 25,80,143,5220

Hvis du ikke skriver inn et portnummer, blir alle portene kontrollert.

IKE-versjon

Velg **IKEv1** eller **IKEv2** for **IKE-versjon**. Velg en av dem avhengig av hvilken enhet skanneren er koblet til.

IKEv1

Følgende elementer vises når du velger **IKEv1** for **IKE-versjon**.

Artikler	Innstillinger og forklaring
Godkjenningmetode	Velg et alternativ hvis du velger IPsec for Tilgangskontroll . Brukt sertifikat er det samme som standardpolicyen.
Forhåndsdelte nøkkel	Hvis du velger Forhåndsdelte nøkkel for Godkjenningmetode , skriver du inn en forhåndsdelte tast på opptil 127 tegn.
Bekreft Forhåndsdelte nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.

IKEv2

Følgende elementer vises når du velger **IKEv2** for **IKE-versjon**.

Artikler		Innstillinger og forklaring
Lokal	Godkjenningstype	Velg et alternativ hvis du velger IPsec for Tilgangskontroll . Brukt sertifikat er det samme som standardpolicyen.
	ID-type	Hvis du velger Forhåndsdelte nøkkel som Godkjenningstype , må du velge ID-typen for skanneren.
	ID	Angi skannerens ID, som samsvarer med ID-typen. Du kan ikke bruke «@», «#» eller «=» som første tegn. Unikt navn: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «=». IP-adresse: Angi format, enten IPv4 eller IPv6. FQDN: Skriv inn en kombinasjon av mellom 1 og 255 tegn med A–Z, a–z, 0–9, «-», og punktum (.). E-postadresse: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «@». Nøkkel-ID: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Forhåndsdelte nøkkel	Hvis du velger Forhåndsdelte nøkkel for Godkjenningstype , skriver du inn en forhåndsdelte tast på opptil 127 tegn.
	Bekreft Forhåndsdelte nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.
Ekstern	Godkjenningstype	Velg et alternativ hvis du velger IPsec for Tilgangskontroll . Brukt sertifikat er det samme som standardpolicyen.
	ID-type	Hvis du velger Forhåndsdelte nøkkel som Godkjenningstype , må du velge ID-type for enheten du vil godkjenne.
	ID	Angi skannerens ID, som samsvarer med ID-type. Du kan ikke bruke «@», «#» eller «=» som første tegn. Unikt navn: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «=». IP-adresse: Angi format, enten IPv4 eller IPv6. FQDN: Skriv inn en kombinasjon av mellom 1 og 255 tegn med A–Z, a–z, 0–9, «-», og punktum (.). E-postadresse: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E). ID-en må inneholde «@». Nøkkel-ID: Skriv inn 1 til 255 enkeltbyte ASCII-tegn (0x20 til 0x7E).
	Forhåndsdelte nøkkel	Hvis du velger Forhåndsdelte nøkkel for Godkjenningstype , skriver du inn en forhåndsdelte tast på opptil 127 tegn.
	Bekreft Forhåndsdelte nøkkel	Skriv inn tasten du konfigurerte for bekreftelse.

Innkapsling

Velger du **IPsec** for **Tilgangskontroll**, må du konfigurere en innkapslingsmodus.

Artikler	Innstillinger og forklaring
Transportmodus	Velg dette hvis du bare bruker skanneren på samme LAN. IP-pakker med lag 4 eller nyere blir kryptert.
Tunnelmodus	Hvis du bruker skanneren på et nettverk som kan kobles til Internett, slik som IPsec-VPN, velg dette alternativet. Toppteksten og dataene i IP-pakkene blir kryptert. Ekstern gateway (Tunnelmodus): Hvis du velger Tunnelmodus for Innkapsling , skriver du inn en gateway-adresse på mellom 1 og 39 tegn.

Sikkerhetsprotokoll

Velg et alternativ hvis du velger **IPsec** for **Tilgangskontroll**.

Artikler	Innstillinger og forklaring
ESP	Velg dette for å sikre integriteten til en godkjenning og dataene, samt kryptere data.
AH	Velg dette for å sikre integriteten til en godkjenning og dataene. Du kan bruke IPsec selv om det er forbudt å kryptere data.

Algoritmeinnstillinger

Det anbefales at du velger **Enhver** for alle innstillinger, eller velger et annet element enn **Enhver** for hver innstilling. Hvis du velger **Enhver** for enkelte innstillinger, og velger et annet element enn **Enhver** for de andre innstillingene, kan enheten muligens ikke kommunisere, avhengig av den andre enheten du vil godkjenne.

Artikler	Innstillinger og forklaring	
IKE	Kryptering	Velg krypteringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
	Godkjenning	Velg godkjenningsalgoritme for IKE.
	Nøkkelutveksling	Velg nøkkelendringsalgoritme for IKE. Elementene vil variere avhengig av IKE-versjon.
ESP	Kryptering	Velg krypteringsalgoritme for ESP. Dette er tilgjengelig når ESP er valgt for Sikkerhetsprotokoll .
	Godkjenning	Velg godkjenningsalgoritme for ESP. Dette er tilgjengelig når ESP er valgt for Sikkerhetsprotokoll .
AH	Godkjenning	Velg krypteringsalgoritme for AH. Dette er tilgjengelig når AH er valgt for Sikkerhetsprotokoll .

Kombinasjon av Lokal adresse (skanner) og Ekstern adresse (vert) på Gruppolicy

	Innstilling av Lokal adresse (skanner)		
	IPv4	IPv6* ²	Alle adresser* ³

Innstilling av Ekstern adresse (vert)	IPv4* ¹	✓	–	✓
	IPv6* ¹ * ²	–	✓	✓
	Tom	✓	✓	✓

*1 Hvis **IPsec** er valgt for **Tilgangskontroll**, kan du ikke spesifisere i en prefikslengde.

*2 Hvis **IPsec** er valgt for **Tilgangskontroll**, kan du velge en link-lokal-adresse (fe80::), men gruppepolicy vil deaktiveres.

*3 Utenom IPv6-link-lokal-adresser.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Referanser for tjenesteneavn på gruppepolicy

Merknad:

Utilgjengelige tjenester vil vises men kan ikke velges.

Tjenesteneavn	Protokolltype	Lokalt portnummer	Eksternt portnummer	Kontrollerte funksjoner
Enhver	–	–	–	Alle tjenester
ENPC	UDP	3289	Hvilken som helst port	Søker etter en skanner fra programmer slik som Epson Device Admin og så en skannerdriver
SNMP	UDP	161	Hvilken som helst port	Henter og konfigurerer MIB fra programmer slik som Epson Device Admin og Epson-skannerdriveren
WSD	TCP	Hvilken som helst port	5357	Kontrollerer WSD
WS-Discovery	UDP	3702	Hvilken som helst port	Søker etter WSD-skannere
Network Scan	TCP	1865	Hvilken som helst port	Videresender skannede data fra Document Capture Pro
Network Push Scan	TCP	Hvilken som helst port	2968	Henter jobbinformasjon for push-skanning fra Document Capture Pro
Network Push Scan Discovery	UDP	2968	Hvilken som helst port	Søke etter en datamaskin fra skanner
FTP-data (ekstern)	TCP	Hvilken som helst port	20	FTP-klient (videresender skannede data) Denne kan imidlertid bare kontrollere en FTP-server som bruker eksternt portnummer 20.
FTP-kontroll (ekstern)	TCP	Hvilken som helst port	21	FTP-klient (kontrollerer videresendte skannede data)

Tjenestenavn	Protokolltype	Lokalt portnummer	Eksternt portnummer	Kontrollerte funksjoner
CIFS (ekstern)	TCP	Hvilken som helst port	445	CIFS-klient (videresender skannede data til en mappe)
NetBIOS Name Service (ekstern)	UDP	Hvilken som helst port	137	CIFS-klient (videresender skannede data til en mappe)
NetBIOS Datagram Service (ekstern)	UDP	Hvilken som helst port	138	
NetBIOS Session Service (ekstern)	TCP	Hvilken som helst port	139	
HTTP (lokal)	TCP	80	Hvilken som helst port	HTTP(S)-server (videresender data fra Web Config og WSD)
HTTPS (lokal)	TCP	443	Hvilken som helst port	
HTTP (ekstern)	TCP	Hvilken som helst port	80	HTTP(S)-klient (oppdaterer fastvaren og rotsertifikatet)
HTTPS (ekstern)	TCP	Hvilken som helst port	443	

Eksempler på IPsec/IP-filtrering

Mottar kun IPsec-pakker

Dette eksemplet viser kun hvordan du konfigurerer en standardpolicy.

Standardpolicy:

- IPsec/IP-filtrering: Aktiver
- Tilgangskontroll: IPsec
- Godkjenningstype: Forhåndsdelte nøkler
- Forhåndsdelte nøkler: Skriv inn opptil 127 tegn.

Gruppestandardpolicy: Skal ikke konfigureres.

Mottar skannerdata og skanneinnstillinger

Dette eksemplet tillater kommunikasjon av skannerdata og skannerkonfigurasjon fra spesifiserte skannere.

Standardpolicy:

- IPsec/IP-filtrering: Aktiver
- Tilgangskontroll: Nekt tilgang

Gruppestandardpolicy:

- Deaktiver denne Gruppestandardpolicy: Merk av for dette alternativet.
- Tilgangskontroll: Gi tilgang
- Ekstern adresse (vert): IP-adresse til en klient

- Metode for å velge port: Tjenestenavn
- Tjenestenavn: Huk av boksen for ENPC, SNMP, HTTP (lokal), HTTPS (lokal) og Network Scan.

Få tilgang kun fra en angitt IP-adresse

Dette eksemplet tillater at en angitt IP-adresse får tilgang til skanneren.

Standardpolicy:

- IPsec/IP-filtrering: Aktiver
- Tilgangskontroll: Nekt tilgang

Gruppolicy:

- Deaktiver denne Gruppolicy: Merk av for dette alternativet.
- Tilgangskontroll: Gi tilgang
- Ekstern adresse (vert): IP-adresse til en administrators klient

Merknad:

Uavhengig av policykonfigurasjonen vil klienten kunne få tilgang til og konfigurere skanneren.

Konfigurere et sertifikat for IPsec/IP-filtrering

Konfigurer klientsertifikat for IPsec/IP-filtrering. Når du angir det, kan du bruke sertifikatet som en godkjenning metode for IPsec/IP-filtrering. Hvis du vil konfigurere sertifiseringsinstans, går du til **CA-sertifikat**.

1. Gå inn på Web Config og velg deretter **Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Klientsertifikat**.
2. Importer sertifikatet i **Klientsertifikat**.
Hvis du allerede har importert et sertifikat utgitt av en sertifiseringsinstans, kan du kopiere sertifikatet og bruke det i IPsec/IP-filtrering. Slik kopierer du det: Velg sertifikatet fra **Kopier fra**, og klikk deretter på **Kopi**.

Relatert informasjon

- ➔ [“Slik kjører du Web Config i en nettleser”](#) på side 37
- ➔ [“Konfigurere et CA-signert sertifikat”](#) på side 92
- ➔ [“Konfigurere et CA-sertifikat”](#) på side 96

Koble skanneren til et IEEE802.1X-nettverk

Konfigurere et IEEE 802.1X-nettverk

Når du angir IEEE 802.1X til skanneren, kan du bruke det på nettverket koblet til en RADIUS-server, en LAN-bryter med godkjenningfunksjon eller et tilgangspunkt.

1. Gå inn på Web Config, og velg deretter **Nettverkssikkerhet**-fanen > **IEEE802.1X** > **Grunnleggende**.

2. Angi en verdi for hvert element.

Hvis du vil bruke skanneren på et trådløst nettverk, klikk på **Wi-Fi-konfigurering** og velg eller fyll inn en SSID.

Merknad:

Du kan dele innstillingene mellom Ethernet og Wi-Fi.

3. Klikk på **Neste**.

Det vises en bekreftelsesmelding.

4. Klikk på **OK**.

Skanneren er oppdatert.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Innstillingselementer for IEEE 802.1X-nettverk

Artikler	Innstillinger og forklaring	
IEEE802.1X (kablet LAN)	Du kan aktivere eller deaktivere innstillingene på siden (IEEE802.1X > Grunnleggende) for IEEE802.1X (kablet LAN).	
IEEE802.1X (Wi-Fi)	Tilkoblingsstatusen for IEEE802.1X (Wi-Fi) vises.	
Tilkoblingsmetode	Tilkoblingsmetoden for gjeldende nettverk vises.	
EAP-type	Velg et alternativ for en godkjenningmetode mellom skanneren og en RADIUS-server.	
	EAP-TLS	Du må få tak i og importere et CA-signert sertifikat.
	PEAP-TLS	
	PEAP/MSCHAPv2	Du må konfigurere et passord.
	EAP-TTLS	
Bruker-ID	Konfigurer en ID som skal brukes som godkjenning av en RADIUS-server. Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).	
Passord	Konfigurer et passord for å godkjenne skanneren. Skriv inn 1 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E). Hvis du bruker en Windows-server som en RADIUS-server, kan du angi opptil 127 tegn.	
Bekreft passord	Skriv inn passordet du konfigurerte som bekreftelse.	
Server-ID	Du kan konfigurere en server-ID for å godkjenne med en bestemt RADIUS-server. Godkjenner bekrefter om det finnes en server-ID i feltet subject/subjectAltName til et serversertifikat som er sendt fra en RADIUS-server. Skriv inn 0 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).	
Sertifikatvalidering (kablet LAN)	Hvis du vil utføre Sertifikatvalidering med IEEE802.1X (kablet LAN) , velger du Aktiver . Hvis du velger Aktiver, må du se den relaterte informasjonen og importere CA-sertifikat . Merk at Sertifikatvalidering alltid er aktivert i IEEE802.1X (Wi-Fi). Husk å importere CA-sertifikat.	

Artikler	Innstillinger og forklaring	
Anonymt navn	Hvis du velger PEAP-TLS eller PEAP/MSCHAPv2 for EAP-type , kan du konfigurere et anonymt navn i stedet for en bruker-ID for fase 1 i en PEAP-godkjenning. Skriv inn 0 til 128 enkeltbyte ASCII-tegn (0x20 til 0x7E).	
Krypteringsstyrke	Du kan velge én av følgende.	
	Høy	AES256/3DES
	Middels	AES256/3DES/AES128/RC4

Relatert informasjon

➔ [“Konfigurere et CA-sertifikat” på side 96](#)

Konfigurere et sertifikat for IEEE 802.1X

Konfigurer klientsertifikat for IEEE802.1X. Når du angir det, kan du bruke **EAP-TLS** og **PEAP-TLS** som godkjenningstype for IEEE 802.1X. Hvis du vil konfigurere sertifiseringsinstanssertifikatet, går du til **CA-sertifikat**.

- Gå inn på Web Config og velg deretter **Nettverkssikkerhet**-fanen > **IEEE802.1X** > **Klientsertifikat**.
- Angi et sertifikat i **Klientsertifikat**.
Hvis du allerede har importert et sertifikat utgitt av en sertifiseringsinstans, kan du kopiere sertifikatet og bruke det i IEEE802.1X. Slik kopierer du det: Velg sertifikatet fra **Kopier fra**, og klikk deretter på **Kopi**.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Løse problemer med avanserte sikkerhetsinnstillinger

Gjenopprette sikkerhetsinnstillingene

Når du oppretter et svært sikkert miljø slik som IPsec/IP-filtrering, vil du kanskje ikke være i stand til å kommunisere med enheter på grunn av feil innstillinger eller problemer med enheten eller serveren. I dette tilfellet, gjenoppretter du sikkerhetsinnstillingene for å foreta innstillinger av enheten på nytt eller muliggjøre midlertidig bruk.

Deaktivere sikkerhetsfunksjonen med Web Config

Du kan deaktivere IPsec/IP-filtrering med Web Config.

- Gå inn på Web Config og velg **Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende**.
- Deaktiver **IPsec/IP-filtrering**.

Problemer ved bruk av funksjoner for nettverkssikkerhet

Glemt en forhåndsdelte tast

Konfigurer en forhåndsdelte tast på nytt.

For å endre tasten, gå inn på Web Config og velg **Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende** > **Standardpolicy** eller **Gruppepolicy**.

Når du endrer den forhåndsdelte nøkkelen, konfigurere den forhåndsdelte nøkkelen for datamaskiner.

Relatert informasjon

- ➔ [“Slik kjører du Web Config i en nettleser”](#) på side 37
- ➔ [“Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering”](#) på side 98

Kan ikke kommunisere med IPsec-kommunikasjon

Spesifiser algoritmen som skanneren eller datamaskinen ikke støtter.

Skanneren støtter følgende algoritmer. Kontroller innstillingene på datamaskinen.

Sikkerhetsmetoder	Algoritmer
IKE-krypteringsalgoritme	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
IKE-godkjenningalgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5
IKE nøkkelendringalgoritme	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
ESP-krypteringsalgoritme	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
ESP-godkjenningalgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5
AH-godkjenningalgoritme	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* kun tilgjengelig for IKEv2

Relatert informasjon

- ➔ [“Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering”](#) på side 98

Kan plutselig ikke kommunisere

Skannerens IP-adresse har blitt endret eller kan ikke brukes.

Når IP-adressen registrert til den lokale adressen på Gruppepolicy har blitt endret eller ikke kan brukes, kan ikke IPsec-kommunisering gjennomføres. Deaktiver IPsec via skannerens kontrollpanel.

Hvis DHCP er utgått, eller omstart eller IPv6-adresse er utgått eller ikke har blitt hentet, vil IP-adressen som er registrert i skannerens Web Config (**Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende** > **Gruppepolicy** > **Lokal adresse (skanner)**), kanskje ikke bli oppdaget.

Bruk en statisk IP-adresse.

Datamaskinens IP-adresse har blitt endret eller kan ikke brukes.

Når IP-adressen registrert til den eksterne adressen på Gruppepolicy har blitt endret eller ikke kan brukes, kan ikke IPsec-kommunisering gjennomføres.

Deaktiver IPsec via skannerens kontrollpanel.

Hvis DHCP er utgått, eller omstart eller IPv6-adresse er utgått eller ikke har blitt hentet, vil IP-adressen som er registrert i skannerens Web Config (**Nettverkssikkerhet**-fanen > **IPsec/IP-filtrering** > **Grunnleggende** > **Gruppepolicy** > **Ekstern adresse (vert)**), kanskje ikke bli oppdaget.

Bruk en statisk IP-adresse.

Relatert informasjon

- ➔ [“Slik kjører du Web Config i en nettleser”](#) på side 37
- ➔ [“Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering”](#) på side 98

Kan ikke koble til etter konfigurering av IPsec/IP-filtrering

Innstillingene til IPsec/IP-filtrering er feil.

Deaktiver IPsec/IP-filtrering via skannerens kontrollpanel. Koble sammen skanneren og datamaskinen og still inn IPsec/IP-filtrering på nytt.

Relatert informasjon

- ➔ [“Kryptert kommunikasjon ved bruk av IPsec/IP-filtrering”](#) på side 98

Får ikke tilgang til enheten etter konfigurering av IEEE 802.1X

Innstillingene til IEEE 802.1X er feil.

Deaktiver IEEE 802.1X og Wi-Fi fra skannerens kontrollpanel. Koble til skanneren og en datamaskin, og konfigurere deretter IEEE 802.1X igjen.

Relatert informasjon

- ➔ [“Konfigurere et IEEE 802.1X-nettverk”](#) på side 109

Problemer med å bruke et digitalt sertifikat

Kan ikke importere et CA-signert sertifikat

CA-signert sertifikat og informasjonen på CSR samsvarer ikke.

Hvis CA-signert sertifikat og CSR-en ikke har samme informasjon, kan ikke CSR importeres. Kontroller følgende:

- Prøver du å importere sertifikatet til en enhet som ikke har den samme informasjonen?
Kontroller informasjonen til CSR-en, og importer deretter sertifikatet til en enhet som har samme informasjon.
- Overskrev du CSR-en som var lagret på skanneren etter at du sendte CSR-en til sertifiseringsinstansen?
Hent det CA-signerte sertifikatet på nytt med CSR-en.

CA-signert sertifikat er mer enn 5 kB.

Du kan ikke importere et CA-signert sertifikat som er større enn 5 kB.

Passordet for å importere sertifikatet er feil.

Oppgi riktig passord. Hvis du glemmer passordet, kan du ikke importere sertifikatet. Innhent CA-signert sertifikat på nytt.

Relatert informasjon

➔ [“Importere et CA-signert sertifikat” på side 94](#)

Kan ikke oppdatere et selvsignert sertifikat

Vanlig navn har ikke blitt skrevet inn.

Vanlig navn må være angitt.

Det har blitt skrevet inn tegn i Vanlig navn som ikke støttes.

Skriv inn mellom 1 og 128 tegn med enten IPv4, IPv6, vertsnavn eller FQDN-format i ASCII (0x20–0x7E).

Det finnes komma eller mellomrom i fellesnavnet.

Hvis du har skrevet inn et komma, vil **Vanlig navn** være delt på det stedet. Det oppstår en feil hvis du har skrevet inn bare et mellomrom før eller etter et komma.

Relatert informasjon

➔ [“Oppdatere et selvsignert sertifikat” på side 96](#)

Kan ikke opprette CSR

Vanlig navn har ikke blitt skrevet inn.

Vanlig navn må være angitt.

Det har blitt skrevet inn tegn i Vanlig navn, Organisasjon, Organisasjonsenhet, Beliggenhet og Stat/provins som ikke støttes.

Skriv inn tegn med enten IPv4, IPv6, vertsnavn eller FQDN-format i ASCII (0x20–0x7E).

Det finnes komma eller mellomrom i Vanlig navn.

Hvis du har skrevet inn et komma, vil **Vanlig navn** være delt på det stedet. Det oppstår en feil hvis du har skrevet inn bare et mellomrom før eller etter et komma.

Relatert informasjon

➔ [“Hente et CA-signert sertifikat” på side 92](#)

Det vises en advarsel om digitalt sertifikat

Meldinger	Årsak/Dette skal du gjøre
Skriv inn et Serversertifikat.	Årsak: Du har ikke valgt hvilken fil som skal importeres. Dette skal du gjøre: Velg filen, og klikk Importer .
CA-sertifikat 1 er ikke angitt.	Årsak: CA-sertifikat 1 er ikke angitt, og kun CA-sertifikat 2 er angitt. Dette skal du gjøre: Importer CA-sertifikat 1 først.
Ugyldig verdi nedenfor.	Årsak: Filbanen og/eller passordet inneholder tegn som ikke støttes. Dette skal du gjøre: Kontroller at tegnene er riktig angitt for elementet.
Ugyldig dato og klokkeslett.	Årsak: Dato og klokkeslett for skanneren er ikke angitt. Dette skal du gjøre: Angi dato og klokkeslett ved hjelp av Web Config eller EpsonNet Config.
Ugyldig passord.	Årsak: Passordet som er angitt for CA-sertifikatet og angitt passord samsvarer ikke. Dette skal du gjøre: Skriv inn riktig passord.

Meldinger	Årsak/Dette skal du gjøre
Ugyldig fil.	<p>Årsak:</p> <p>Du importerer ikke en sertifikatfil i X509-format.</p> <p>Dette skal du gjøre:</p> <p>Kontroller at du velger riktig sertifikat som er sendt fra en klarert sertifiseringsinstans.</p>
	<p>Årsak:</p> <p>Filen du har importert er for stor. Maksimal filstørrelse er 5 kB.</p> <p>Dette skal du gjøre:</p> <p>Hvis du velger riktig fil, kan sertifikatet bli skadet eller forfalsket.</p>
	<p>Årsak:</p> <p>Kjeden i sertifikatet er ugyldig.</p> <p>Dette skal du gjøre:</p> <p>Du finner mer informasjon om sertifikatet på nettstedet til sertifiseringsinstansen.</p>
Kan ikke bruke Serversertifikater som inkluderer mer enn tre CA-sertifikater.	<p>Årsak:</p> <p>Sertifikatfilen i PKCS#12-format inneholder mer enn 3 CA-sertifikater.</p> <p>Dette skal du gjøre:</p> <p>Importer hvert enkelt sertifikat ved å konvertere dem fra PKCS#12-format til PEM-format, eller importer sertifikatfilen i PKCS#12-format som inneholder opptil 2 CA-sertifikater.</p>
Sertifikatet er utløpt. Kontroller at sertifikatet er gyldig, eller kontroller dato og klokkeslett på produktet.	<p>Årsak:</p> <p>Sertifikatet er foreldet.</p> <p>Dette skal du gjøre:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Hvis sertifikatet er foreldet, må du hente og importere det nye sertifikatet. <input type="checkbox"/> Hvis sertifikatet ikke er foreldet, kontrollerer du at skannerens dato og klokkeslett er riktig angitt.
Privat nøkkel kreves.	<p>Årsak:</p> <p>Det finnes ingen paret privatnøkkel med sertifikatet.</p> <p>Dette skal du gjøre:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Hvis sertifikatet er i PEM/DER-format og det er hentet fra en CSR ved hjelp av en datamaskin, angir du filen for privatnøkkelen. <input type="checkbox"/> Hvis sertifikatet er i PKCS#12-format og det er hentet fra en CSR ved hjelp av en datamaskin, oppretter du en fil som inneholder privatnøkkelen.
	<p>Årsak:</p> <p>Du har importert PEM/DER-sertifikatet du hentet fra en CSR på nytt ved hjelp av Web Config.</p> <p>Dette skal du gjøre:</p> <p>Hvis sertifikatet er i PEM/DER-format og det er hentet fra en CSR ved hjelp av Web Config, kan du bare importere det én gang.</p>

Meldinger	Årsak/Dette skal du gjøre
Innstilling mislykket.	<p>Årsak:</p> <p>Kan ikke fullføre konfigurasjonen fordi kommunikasjonen mellom skanneren og datamaskinen mislyktes eller filen ikke kan leses pga. feil.</p> <p>Dette skal du gjøre:</p> <p>Når du har kontrollert angitt fil og kommunikasjon, importerer du filen på nytt.</p>

Relatert informasjon

➔ [“Om digital sertifisering” på side 92](#)

Slette et CA-signert sertifikat ved et uhell

Det finnes ingen sikkerhetskopifil for det CA-signerte sertifikatet.

Hvis du har sikkerhetskopifilen, kan du importere sertifikatet på nytt.

Hvis du henter et sertifikat med en CSR som er opprettet fra Web Config, kan du ikke importere et slettet sertifikat på nytt. Opprett en CSR, og hent et nytt sertifikat.

Relatert informasjon

➔ [“Importere et CA-signert sertifikat” på side 94](#)

➔ [“Slette et CA-signert sertifikat” på side 95](#)

Bruke Epson Open Platform

Oversikt over Epson Open Platform.	119
Konfigurere Epson Open Platform.	119
Bekreftede Epson Open Platform.	119

Oversikt over Epson Open Platform

Epson Open Platform er en plattform som lar deg bruke autentiseringssystemer med denne skanneren.

Den kan brukes med Epson Print Admin (Epsons godkjenningssystem) eller et godkjenningssystem fra en tredjepart. Du kan finne logger om enheten og brukere, konfigurere enheter som kan brukes av bestemte brukere og grupper, angi grenser for funksjonene og så videre.

Hvis du kobler til en godkjenningseenhet, kan du også utføre brukergodkjenning med ID-kortet.

Konfigurere Epson Open Platform

Aktiver Epson Open Platform slik at du kan bruke enheten fra godkjenningssystemet.

1. Få en produktnøkkel fra det dedikerte nettstedet.
Se Epson Open Platform-håndboken for mer informasjon om hvordan du finner produktnøkkelen.
2. Åpne Web Config og velg **Epson Open Platform**-fanen > **Produktnøkkel eller Lisensnøkkel**.
3. Sjekk og still inn hvert element.
 - Serienummer
Serienummeret for enheten vises.
 - Epson Open Platform-versjon
Velg versjonen av Epson Open Platform. De samsvarende versjonene varierer avhengig av godkjenningssystemet.
 - Produktnøkkel eller Lisensnøkkel
Skriv inn produktnøkkelen du fikk.
4. Klikk på **Neste**.
Bekreftelseskjerm bildet for innstillinger vises.
5. Klikk på **OK**.
Innstillingene brukes på skanneren.

Merknad:

Du kan ikke bruke Epson Print Admin Serverless når systemet er synkronisert med Epson Open Platform.

Bekrefte Epson Open Platform

Du kan sjekke gyldigheten til Epson Open Platform med en av metodene nedenfor.

- Web Config
Det er angitt en produktnøkkel i **Epson Open Platform**-fanen > **Produktnøkkel eller Lisensnøkkel** > **Produktnøkkel eller Lisensnøkkel**, og **Epson Open Platform**-fanen > **Autentiseringssystem** vises til venstre for menytreet.
- Skannerens kontrollpanel
Kontroller at produktnøkkelen vises i **Innst.** > **Enhetsinformasjon** > **Informasjon om Epson Open Platform**.

Montere en godkjenningseenhet

Koble til en godkjenningseenhet.	121
Driftssjekk for godkjenningseenheter.	121
Bekreft at godkjenningkortet gjenkjennes.	121
Feilsøke godkjenningseenheten.	122

Koble til en godkjenningssenhet

Merknad:

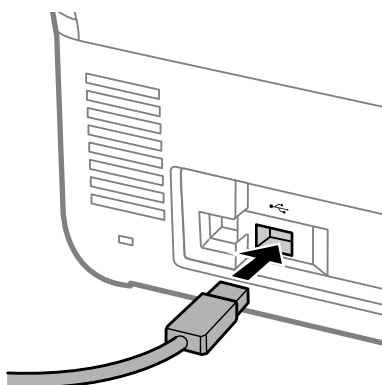
En godkjenningssenhet brukes når du bruker et godkjenningssystem.



Forsiktighetsregel:

Når du kobler godkjenningssenheden til flere skannere, må du bruke et produkt med samme modellnummer.

Koble kortleserens USB-kabel til USB-porten for eksterne grensesnitt på skanneren.



Driftssjekk for godkjenningssenheter

Du kan sjekke tilkoblingsstatusen og gjenkjenning av godkjenningsskortet for godkjenningssenheden fra skannerens kontrollpanel.

Informasjonen vises når du velger **Innst.** > **Enhetsinformasjon** > **Status for godkjenningssenhet**.

Bekrefte at godkjenningsskortet gjenkjennes

Du kan kontrollere at godkjenningsskort gjenkjennes ved hjelp av Web Config.

1. Åpne Web Config og velg **Enhetsadministrasjon**-fanen > **Kortleser**.
2. Hold godkjenningsskortet over kortleseren.
3. Klikk på **Kontroller**.

Resultatet vises.

Feilsøke godkjenningssenheten

Kan ikke lese godkjenningsskortet

Kontroller følgende.

- Sjekk om godkjenningssenheten er koblet riktig til skanneren.
Koble godkjenningssenheten til USB-porten for eksternt grensesnitt på baksiden av skanneren.
- Sjekk at autentiseringssenheten og autentiseringsskortet er sertifisert.
Kontakt forhandleren din for informasjon om støttede autentiseringssenheter og kort.

Vedlikehold


Rengjøre utsiden av skanneren.	124
Rengjøre innsiden av skanneren.	124
Bytte ut rullersetet.	129
Tilbakestill antall skanninger etter å ha byttet ut rullen.	134
Energisparing.	135
Transportere skanneren.	135
Sikkerhetskopier innstillingene.	136
Gjenopprett standardinnst.	137
Oppdatere programmer og fastvare.	138

Rengjøre utsiden av skanneren

Tørk av eventuelle flekker på kabinettet med en tørr klut eller en klut fuktet med mildt rengjøringsmiddel og vann.

 **Forsiktighetsregel:**

- Bruk aldri alkohol, fortynningsmidler eller etsende løsemidler til å rengjøre skanneren. Misdannelse eller misfaring kan oppstå.*
- Ikke la vann tre inn i produktet. Dette kan forårsake en funksjonssvikt.*
- Ikke åpne skannerkabinettet.*

1. Trykk -knappen for å slå av skanneren.
2. Koble AC-adapteren fra skanneren.
3. Rengjør kabinettet med en klut fuktet med et mildt vaskemiddel og vann.

Merknad:

Tørk av berøringsskjermen med en myk, tørr klut.

Rengjøre innsiden av skanneren


Etter å ha brukt skanneren en stund, kan papir og romstøv på rulleren eller glassdelen på innsiden av skanneren forårsake problemer med papirmating eller kvalitet av skannede bilder. Rengjør innsiden av skanneren i intervaller på 5,000 skanninger.

Du kan sjekke siste antall skanninger på kontrollpanelet eller i Epson Scan 2 Utility.

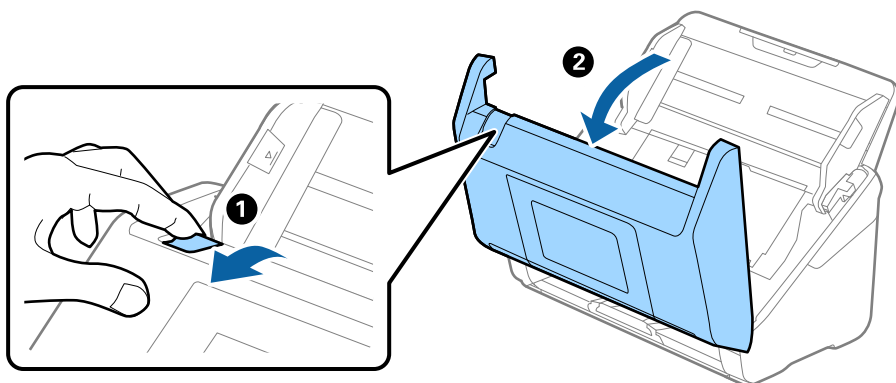
Dersom det har kommet vanskelige flekker på overflaten, bruk et ekte Epson rensesett for å fjerne dem. Bruk en liten mengde rensmiddel på kluten og fjern flekkene.

 **Forsiktighetsregel:**

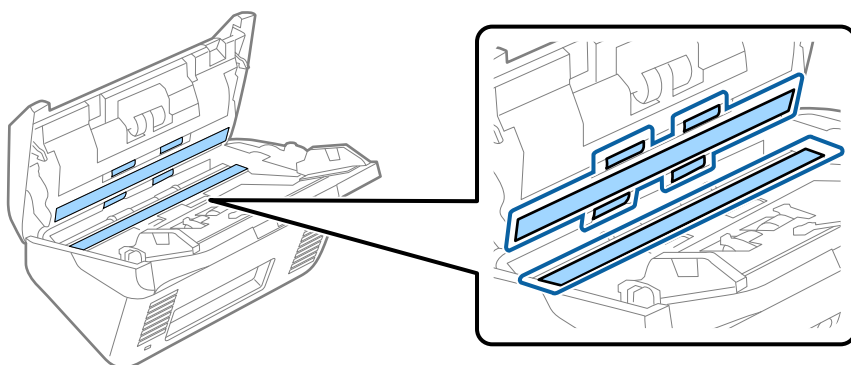
- Bruk aldri alkohol, fortynningsmidler eller etsende løsemidler til å rengjøre skanneren. Misdannelse eller misfaring kan oppstå.*
- Spray aldri væsker eller smøremiddel på skanneren. Skade på utstyr eller kretser kan forårsake unormal drift.*
- Ikke åpne skannerkabinettet.*

1. Trykk -knappen for å slå av skanneren.
2. Koble strømadapteren fra skanneren.

3. Dra i spaken og åpne skannerdekselet.



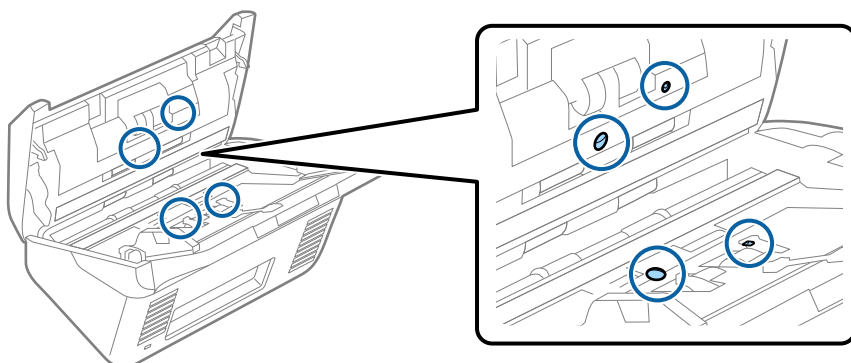
4. Tørk av eventuelle flekker på plastrullen (4 steder) og glassoverflaten på undersiden av skannerdekselet med en myk klut. Tørk med en myk, lofri klut fuktet med en liten mengde dedikert vaskemiddel eller vann.



Forsiktighetsregel:

- Ikke påfør for mye kraft på glassoverflaten.
- Ikke bruk en børste eller et hardt verktøy. Eventuelle skraper på glasset kan påvirke skannekvaliteten.
- Ikke spray rengjøringsmiddel direkte på glassoverflaten.

5. Tørk av eventuelle flekker på sensorene med en bomullspinne.

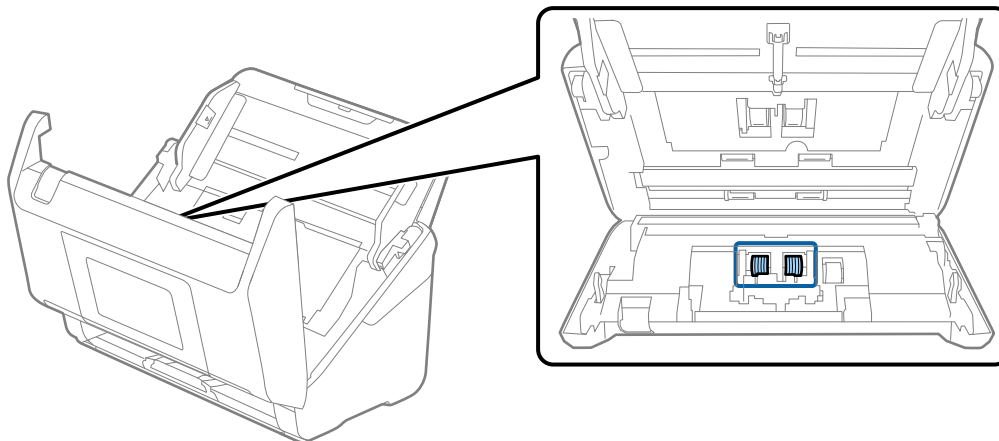




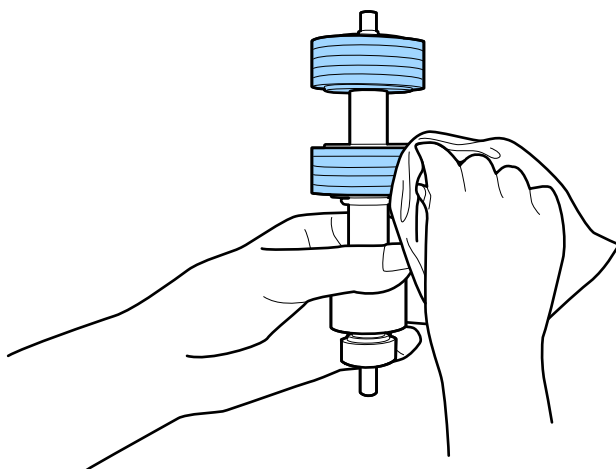
Forsiktighetsregel:

Ikke bruk væsker slik som et rengjøringsmiddel på en bomullspinne.

6. Åpne dekselet og fjern så separasjonsrullen.
Se «Bytte ut rullersetet» for mer informasjon.



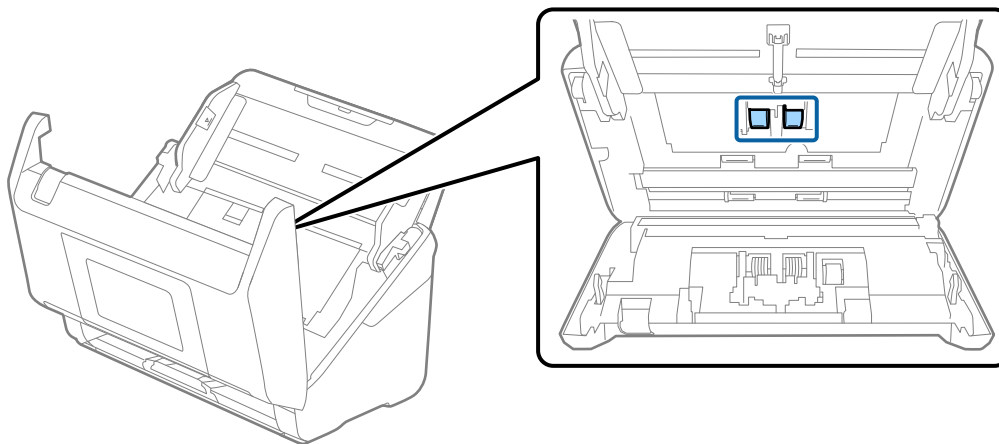
7. Tørk separeringsrullen. Tørk med en myk, lofri klut fuktet med en liten mengde dedikert vaskemiddel eller vann.



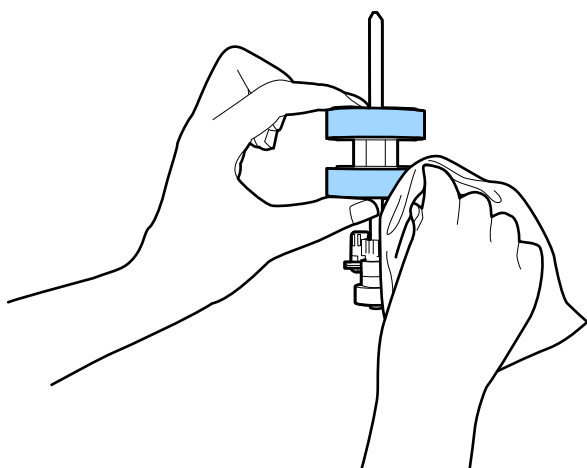
Forsiktighetsregel:

Bruk kun et ekte Epson-rensesett eller en myk, fuktig klut til å rengjøre rullen. Bruk av tørr klut kan skade overflaten av valsen.

8. Åpne dekselet og fjern så oppsamlingsrullen.
Se «Bytte ut rullersetet» for mer informasjon.



9. Tørk pickup-rullen. Tørk med en myk, løfri klut fuktet med en liten mengde dedikert vaskemiddel eller vann.

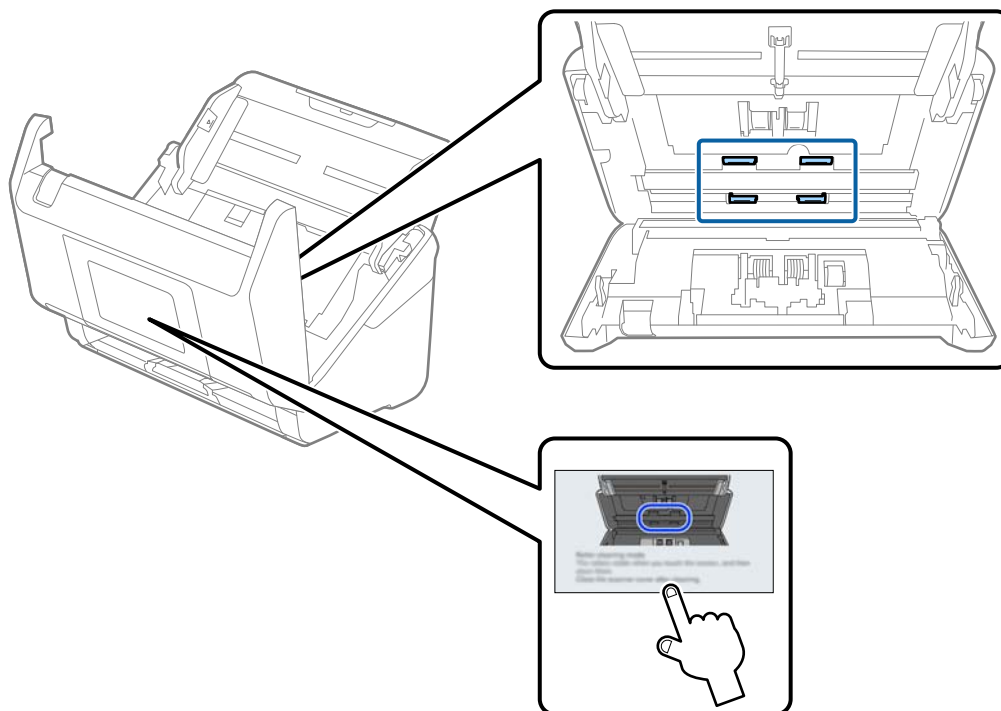


Forsiktighetsregel:

Bruk kun et ekte Epson-rensesett eller en myk, fuktig klut til å rengjøre rullen. Bruk av tørr klut kan skade overflaten av valsen.

10. Lukk skannerdekselet.
11. Sett inn strømadapteren og slå så på skanneren.
12. Velg **Vedlikehold av skanner** fra hjemmeskjermen.
13. Velg **Rengjøring av vals** på **Vedlikehold av skanner** skjermen.
14. Trekk i spaken for å åpne skannerdekslet.
Skanneren går inn i rulle-rengjøringsmodus.

15. Sakte roter rullene i bunnen ved å trykke hvor som helst på skjermen. Tørk av valsene med et ekte Epson-rensesett eller en myk klut fuktet med vann. Gjenta inntil rullene er rengjort.



Forsiktig:

Vær forsiktig så hendene dine eller håret ditt ikke setter seg fast i mekanismen mens du opererer rullen. Dette kan forårsake en ulykke.

16. Lukk skannerdekselet.

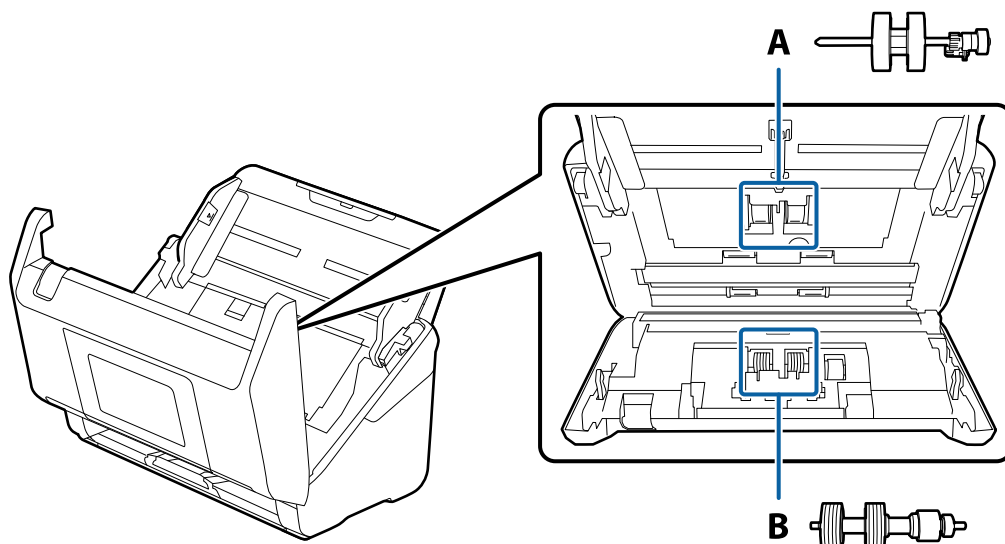
Skanneren går ut av rulle-rengjøringsmodus.

Relatert informasjon


➔ [“Bytte ut rullersettet” på side 129](#)

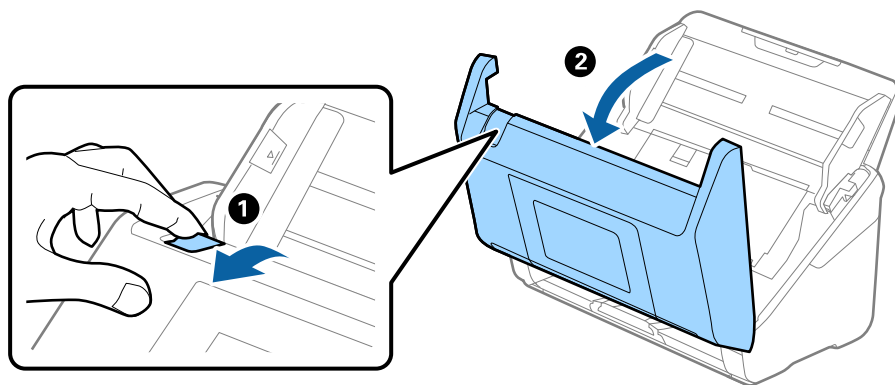
Bytte ut rullersettet

Rullersettet (pickup-rulleren og separeringsrulleren) må byttes ut når antall skanninger overskrider livssyklusen til rullene. Når en erstatningsmelding vises på kontrollpanelet eller dataskjermen, følger du trinnene nedenfor for å erstatte det.

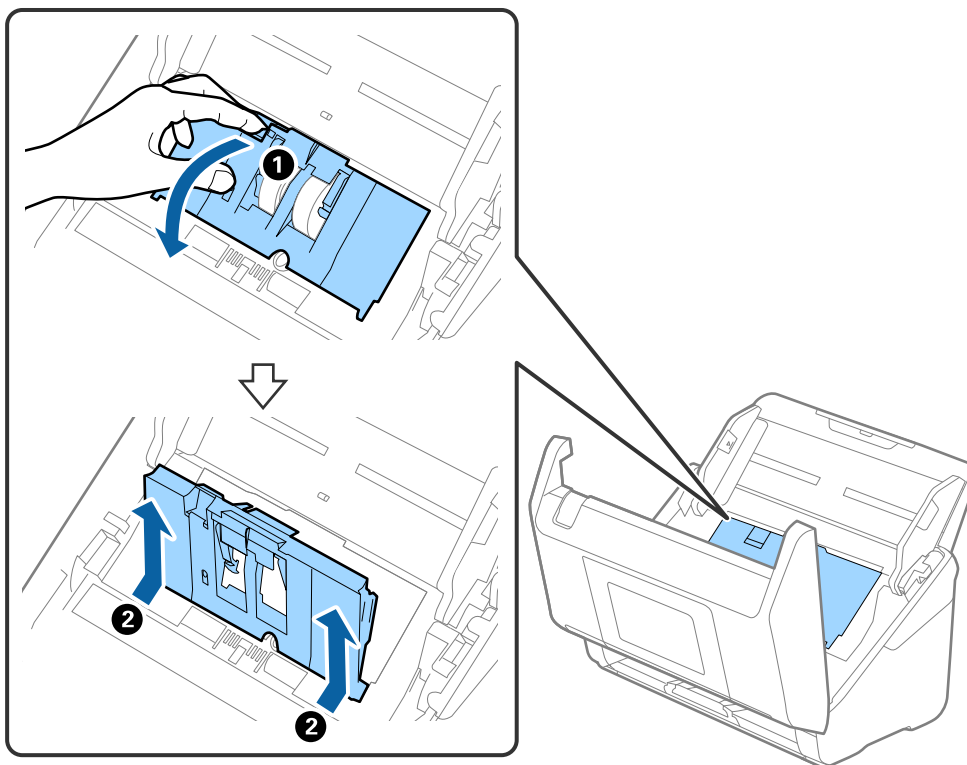


A: pickup-rulle, B: separeringsrulle

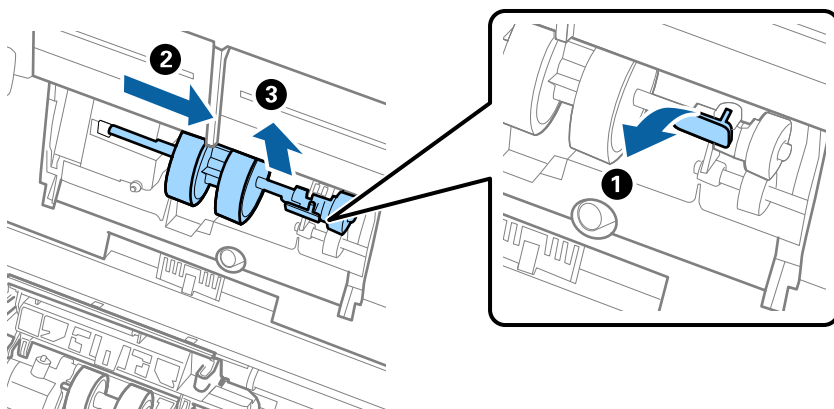
1. Trykk -knappen for å slå av skanneren.
2. Koble AC-adapteren fra skanneren.
3. Dra i spaken og åpne skannerdekselet.



4. Åpne dekselet til oppsamlingsrulleren og så glir og fjerner du den.



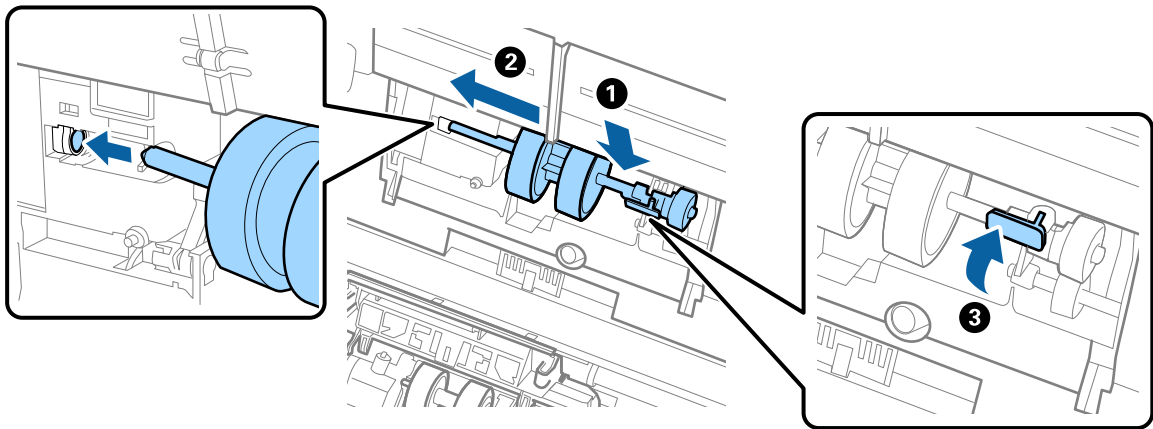
5. Trekk så fiksturen av rulleraksen og så glir du og fjerner de monterte oppsamlingsrullene.



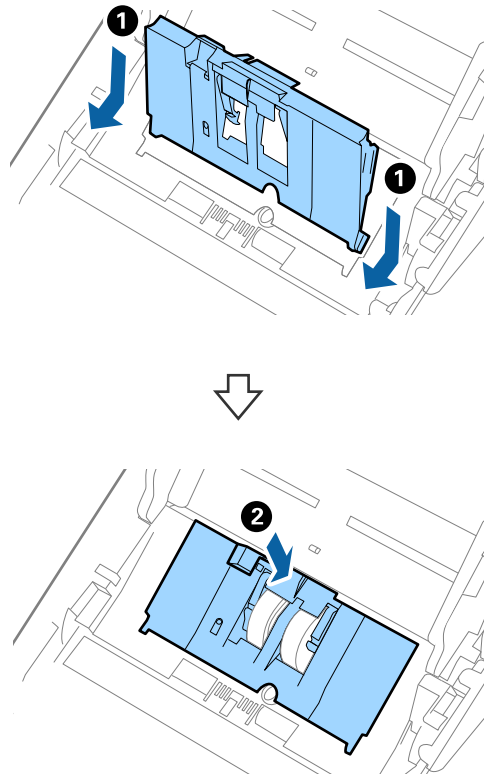
Forsiktighetsregel:

Ikke dra ut oppsamlingsrullen med makt. Dette kan skade innsiden av skanneren.

6. Mens du holder fiksturen nede, glir du den nye oppsamlingsrullen til venstre og setter den inn i hullet i skanneren. Trykk fiksturen for å sikre den.

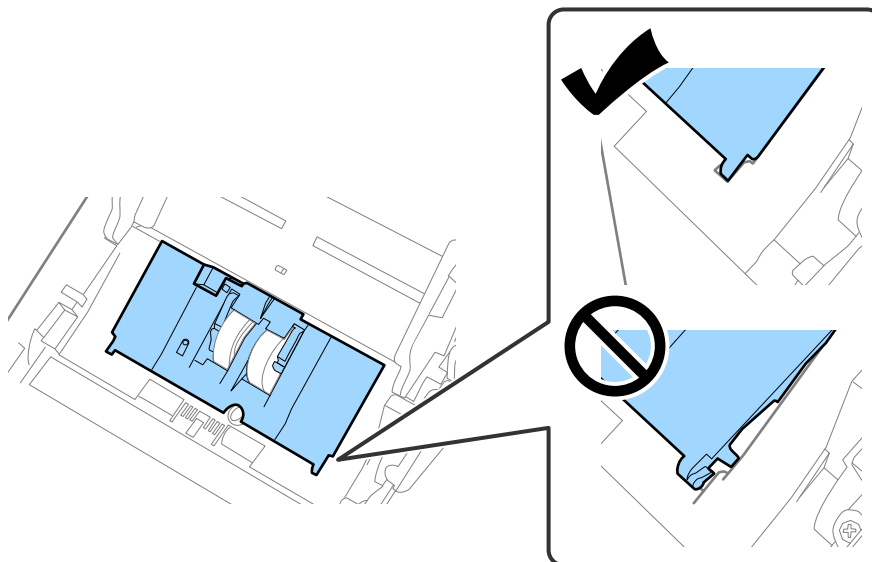


7. Sett kanten av dekselet til oppsamlingsrullen inn i sporet og gli den inn. Lukk dekselet godt.

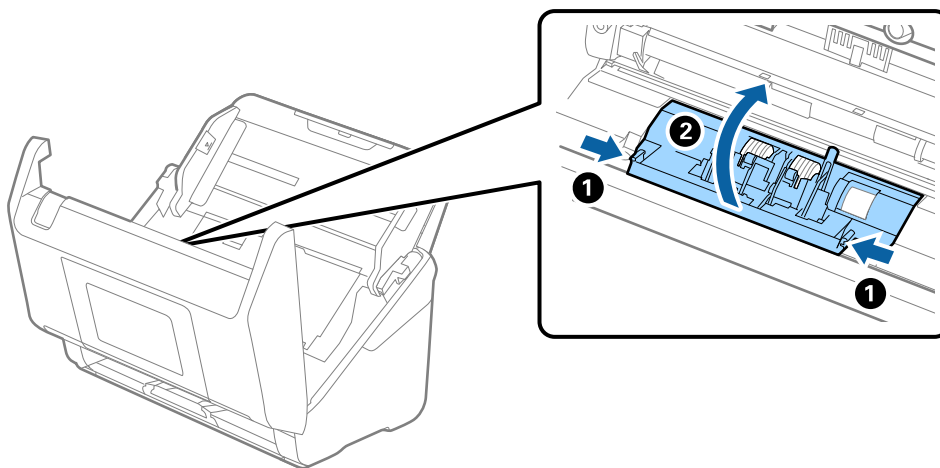


! Forsiktighetsregel:

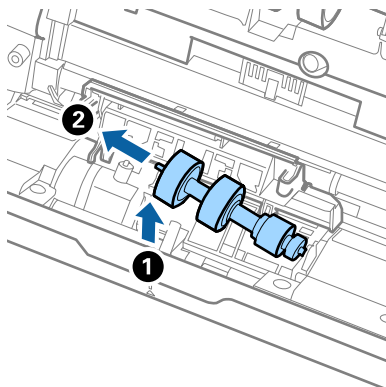
- Sørg for at oppsamlingsdekselet er riktig lukket.
- Kontroller at oppsamlingsrullene er riktig montert hvis det er vanskelig å lukke dekselet.
- Ikke monter dekselet mens det er hevet.



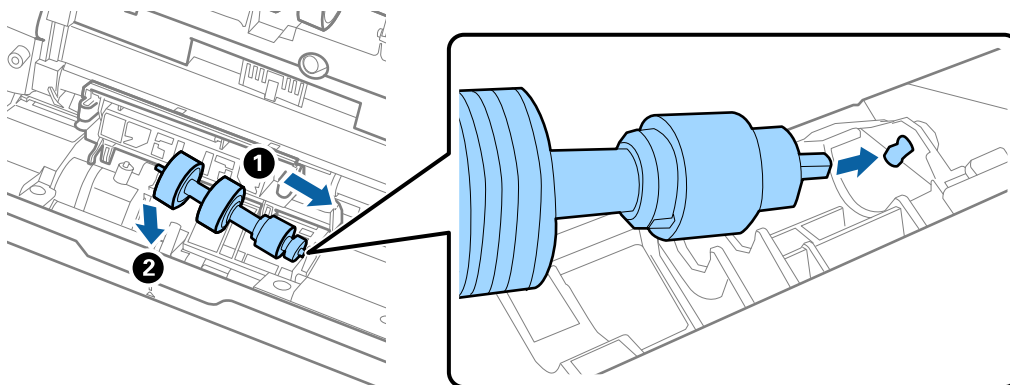
8. Dytt krokene på begge sider av dekselet til oppsamlingsrullen for å åpne dekselet.



9. Løft venstre side av separasjonsrullen og så glir du og fjerner de monterte separasjonsrullene.



10. Sett den nye aksen for separasjonsrullen inn i hullet på høyre side, og så senker du rullen.



11. Lukk dekselet for separasjonsrullen.



Forsiktighetsregel:

Hvis dekselet er vanskelig å lukke, sjekk at separasjonsrullene er riktig installert.

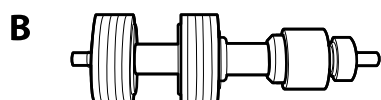
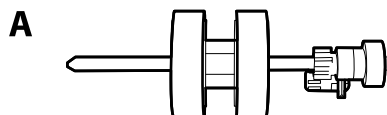
12. Lukk skannerdekselet.
13. Sett inn AC-adapteren og slå så på skanneren.
14. Tilbakestill skanningsantallet på kontrollpanelet.

Merknad:

Avhend oppsamlingsrullen og separasjonsrullen i henhold til lokale regler og bestemmelser. Ikke demonter dem.

Koder for rullersett

Deler (opsamlingsruller og separasjonsruller) bør skiftes når antall skanninger overstiger tjenestenummer. Du kan sjekke siste antall skanninger på kontrollpanelet eller i Epson Scan 2 Utility.



A: oppsamlingsruller, B: separasjonsruller

Delenavn	Koder	Livssyklus
Rullersett 2	B12B819711 B12B819721 (bare India)	200,000*

* Dette antallet ble nådd med etterfølgende skanning med Epson-originalpapir for testing og er en veiledning for utskiftningssyklusen. Utskiftningssyklusen kan avvike avhengig av forskjellige papirtyper, slik som et papir som genererer masse papirstøv eller papir med en ujevn overflate kan forkorte livssyklusen.

Tilbakestill antall skanninger etter å ha byttet ut rullen

Tilbakestill antall skanninger ved hjelp av kontrollpanelet eller Epson Scan 2 Utility etter at du har byttet rullersettet.

Dette avsnittet forklarer hvordan du tilbakestiller med kontrollpanelet.

1. Trykk **Vedlikehold av skanner** på hjemmeskjermen.
2. Trykk **Utskiftning av vedlikeholdsvalse**.
3. Trykk **Tilbakestill antall skanninger**.
4. Velg **Antall skanninger etter valsbytte**, og trykk deretter **Ja**.

Merknad:

For å nullstille Epson Scan 2 Utility, må du starte Epson Scan 2 Utility, klikke på **Telleverk**-fanen og deretter klikke på **Tilbakestill** i **Valsesammensettingspakke**.

Relatert informasjon

➔ [“Bytte ut rullersettet” på side 129](#)

Energisparing

Du kan spare energi ved å bruke hvilemodus eller auto strøm av-modus når ingen operasjoner blir utført av skanneren. Du kan angi tidsperioden før skanneren går inn i hvilemodus og slår seg av automatisk. Økning vil påvirke produktets energieffektivitet. Ta hensyn til miljøet før du gjør noen endringer.


1. Velg **Innst.** på startskjermen.
2. Velg **Basisinnstillinger**.
3. Velg **Innsovingstid** eller **Avslåingsinnst.**, og angi deretter innstillingene.

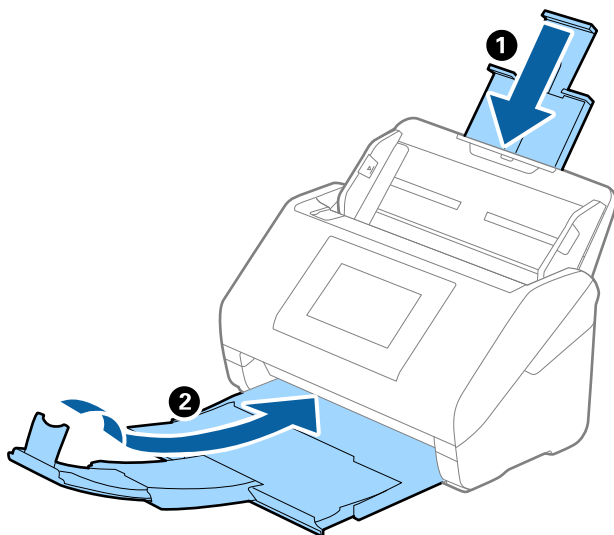
Merknad:

Tilgjengelige funksjoner kan variere avhengig av kjøpssted.

Transportere skanneren

Når du må transportere skanneren pga flytting eller reparasjon, må du følge trinnene under for å pakke skanneren.

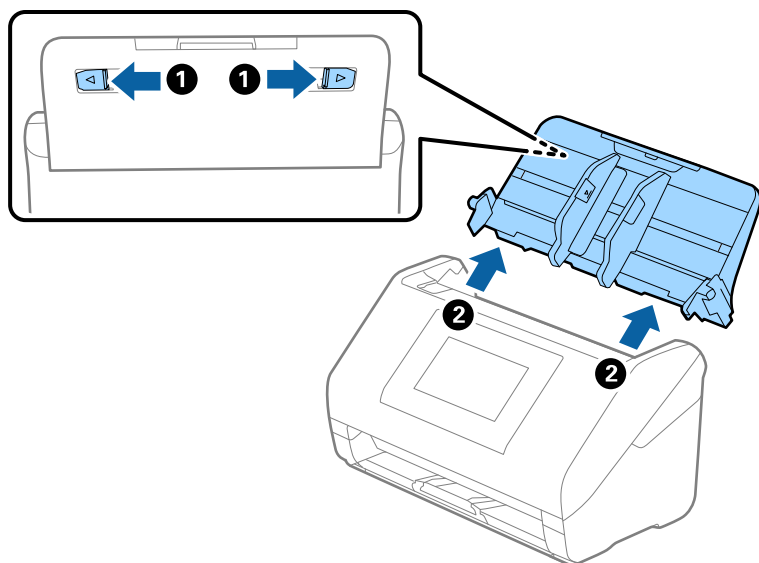
1. Trykk -knappen for å slå av skanneren.
2. Koble fra strømadapteren.
3. Fjern kablene og enhetene.
Fjern Paper Alignment Plate (ekstraustyr eller inkludert) hvis den er festet.
4. Lukk innskuffens forlengelse og utskuffen.



Forsiktighetsregel:

Sørg for at du lukker utskuffen godt, ellers kan den bli skadet under transport.

5. Fjern innskuffen.



6. Fest emballasjen som fulgte med skanneren og pakk deretter skanneren ned igjen i originalesken eller en solid eske.

Sikkerhetskopier innstillingene

Du kan eksportere innstillingsverdien angitt fra Web Config til filen. Du kan bruke den til å sikkerhetskopiere kontaktene, stille inn verdier, bytte skanneren, osv.

Den eksporterte filen kan redigeres fordi den eksporteres som en binær fil.

Eksportere innstillingene

Eksporter innstillingen for skanneren.

1. Gå inn på Web Config, og velg deretter **Enhetsadministrasjon**-fanen > **Innstillingsverdi for eksportering og importering** > **Eksporter**.
2. Velg innstillingene du vil eksportere.
Velg innstillingene du vil eksportere. Hvis du velger en overordnet kategori, velges også underkategorier. Imidlertid kan underkategorier som forårsaker feil ved duplisering innenfor samme nettverk (for eksempel IP-adresser og så videre) ikke velges.
3. Skriv inn et passord for å kryptere den eksporterte filen.
Du trenger passordet for å importere filen. La dette stå tomt hvis du ikke ønsker å kryptere filen.

4. Klikk på **Eksporter**.



Forsiktighetsregel:

*Hvis du vil eksportere nettverksinnstillingene til skanneren, som enhetsnavnet og IPv6-adresse, velger du **Aktiver for å velge individuelle innstillinger for enhet** og velger flere elementer. Bruk bare de valgte verdiene for skanneren som utskiftes.*

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Importere innstillingene

Importer den eksporterte Web Config-filen til skanneren.



Forsiktighetsregel:

Ved import av verdier som inkluderer individuell informasjon, for eksempel skannernavn eller IP-adresse, må du kontrollere at den samme IP-adressen ikke eksisterer på samme nettverk.

1. Åpne Web Config og velg **Enhetsadministrasjon**-fanen > **Innstillingsverdi for eksportering og importering** > **Importer**.
2. Velg den eksporterte filen og skriv deretter inn det krypterte passordet.
3. Klikk på **Neste**.
4. Velg innstillingene du vil importere, og klikk deretter **Neste**.
5. Klikk på **OK**.

Innstillingene brukes på skanneren.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser” på side 37](#)

Gjenoppsett standardinnst.

Velg **Innst.** > **Systemadministrasjon** > **Gjenoppsett standardinnst.** fra kontrollpanelet, og velg deretter elementene du vil gjenopprette til standardinnstillingene.

- Nettverksinnstillinger: gjenopprette nettverksrelaterte innstillinger til deres opprinnelige status.
- Alt unntatt Nettverksinnstillinger: gjenopprette andre innstillinger til sin opprinnelige status unntatt nettverksrelaterte innstillinger.
- Alle innstillinger: gjenopprette alle innstillinger til sin opprinnelige status når kjøpt.



Forsiktighetsregel:

Hvis du velger og kjører **Alle innstillinger**, slettes alle innstillingsdata som er registrert på skanneren, inkludert kontakter. Slettede innstillinger kan ikke gjenopprettes.

Merknad:

Du kan også gjøre innstillinger på Web Config.

Enhetsadministrasjon-fanen > Gjenopprett standardinnstillinger

Oppdatere programmer og fastvare

Du kan bli kvitt visse problemer og forbedre eller legge til funksjoner ved å oppdatere programmene og fastvaren. Forsikre deg om at du bruker den seneste versjonen av programmene og fastvaren.



Forsiktighetsregel:

Ikke slå av datamaskinen eller skanneren under oppdatering.

Merknad:

Når skanneren kan koble til Internett, kan du oppdatere fastvaren via Web Config. Velg **Enhetsadministrasjon-fanen > Fastvareoppdatering**, sjekk meldingen som vises og klikk deretter på **Start**.

1. Kontroller at skanneren og datamaskinen er koblet sammen, og at datamaskinen er koblet til Internett.
2. Start EPSON Software Updater, og oppdater programmene eller fastvaren.

Merknad:

Windows Server-operativsystem støttes ikke.

Windows 11

Klikk startknappen og velg deretter **Alle programmer > Epson Software > EPSON Software Updater**.

Windows 10

Klikk startknappen og velg **Epson Software > EPSON Software Updater**.

Windows 8.1/Windows 8

Angi programvarens navn i søkeboksen og velg deretter det viste ikonet.

Windows 7

Klikk startknappen og velg deretter **Alle programmer** eller **Programmer > Epson Software > EPSON Software Updater**.

Mac OS

Velg **Finder > Gå > Programmer > Epson Software > EPSON Software Updater**.

Merknad:

Hvis du ikke finner programmet du vil oppdatere i listen, kan du ikke oppdatere det ved hjelp av EPSON Software Updater. Se etter seneste versjoner av programmene på Epsons lokale nettside.

<http://www.epson.com>

Oppdatere skannerens fastvare ved hjelp av kontrollpanelet

Hvis skanneren kan bli koblet til Internett, kan du oppdatere skannerens fastvare via kontrollpanelet. Du kan også angi at skanneren jevnlig skal se etter fastvareoppdateringer og varsle deg hvis det er noen.

1. Velg **Innst.** på startskjermen.
2. Velg **Systemadministrasjon > Fastvareoppdatering > Oppdater.**
Merknad:
Velg **Varsel > På** for å angi at skanneren jevnlig skal se etter tilgjengelige fastvareoppdateringer.
3. Se meldingen som vises på skjermen og begynn å søke etter tilgjengelige oppdateringer.
4. Hvis det vises en melding på LCD-skjermen om at det finnes en fastvareoppdatering, følger du instruksjonene på skjermen for å starte oppdateringen.



Forsiktighetsregel:

- Du må ikke slå av eller trekke ut kontakten til skanneren før oppdateringen er fullført, ellers kan det oppstå feil på skanneren.
- Hvis fastvareoppdateringen ikke fullføres eller er vellykket starter ikke skanneren som normalt og meldingen «Recovery Mode» vises på LCD-skjermen neste gang skanneren blir slått på. I så fall må du oppdatere fastvaren på nytt ved hjelp av datamaskinen. Koble skanneren til datamaskinen med en USB-kabel. Når «Recovery Mode» vises på skanneren, kan du ikke oppdatere fastvaren via en nettverkstilkobling. På datamaskinen går du til det lokale nettstedet til Epson, og deretter laster du ned den nyeste skannerfastvaren. Se i instruksjonene på nettstedet for hva du skal gjøre videre.

Oppdatere fastvaren ved å bruke Web Config

Når skanneren kan koble til Internett, kan du oppdatere fastvaren via Web Config.

1. Gå inn på Web Config og velg **Enhetsadministrasjon**-fanen > **Fastvareoppdatering**.
2. Klikk på **Start**, og følg instruksjonene på skjermen.

Fastvarekontrollen starter, og fastvareinformasjonen vises dersom oppdatert fastvare finnes.

Merknad:

Du kan også oppdatere fastvarer ved å bruke Epson Device Admin. Du kan ta en visuell sjekk av fastvareinformasjonen på enhetslisten. Dette er nyttig når du ønsker å oppdatere fastvaren på flere enheter. Se Epson Device Admin-veiledningen for mer informasjon.

Relatert informasjon

➔ [“Slik kjører du Web Config i en nettleser”](#) på side 37

Oppdatere fastvaren uten å koble til Internett

Du kan laste ned enhetens fastvare fra Epson-nettstedet på en datamaskin og deretter koble enheten til datamaskinen med en USB-kabel for å oppdatere fastvaren. If you cannot update over the network, try this method.

Merknad:

Før du oppdaterer må du være sikker på at skannerdriveren Epson Scan 2 er installert på datamaskinen. Hvis Epson Scan 2 ikke er installert, må du installere den på nytt.

1. Sjekk Epsons nettside for å finne de siste utgavene av fastvareoppdateringer.

<http://www.epson.com>

- Hvis det finnes fastvare til skanneren din, må du laste denne ned og gå til neste trinn.
- Hvis det ikke finnes fastvareinformasjon på nettsiden, bruker du allerede den nyeste fastvaren.

2. Koble datamaskinen som fastvaren ble lastet ned til skanneren ved å bruke en USB-kabel.

3. Dobbeltklikk på den nedlastede .exe-filen.

Epson Firmware Updater starter.

4. Følg instruksjonene på skjermen.